VIGILANT
SOLUTIONS

2016-157
DPS CONTRACT NO.

Enterprise Service Agreement (ESA)

This Vigilant Solutions Enterprise Service **Agreement (the "Agreement") is made and entered into as of** this 1st Day of November, 2016 by and between **Vigilant Solutions, LLC**, a Delaware corporation, having its principal place of business at 2021 Las Positas Court Suite # 101, Livermore, CA 94551 ("Vigilant") and AZ Dept of Public Safety, a law enforcement agency (LEA) or other governmental agency, having its principal place of business at 2102 W Encanto Blvd, Phoenix, AZ 85009 ("Affilliate").

WHEREAS, Vigilant designs, develops, licenses and services advanced video analysis software technologies for the law enforcement and security markets;

WHEREAS, Vigilant provides access to license plate data as a value added component of the Vigilant law enforcement package of license plate recognition equipment and software;

WHEREAS, Affiliate will separately purchase License Plate Recognition (LPR) hardware components from Vigilant and/or its authorized reseller for use with the Software Products (as defined below);

WHEREAS, Affiliate desires to license from and receive service for the Software Products provided by Vigilant;

THEREFORE, In consideration of the mutual covenants contained herein this Agreement, Affiliate and Vigilant hereby agree as follows:

I. Definitions:

"CLK" or **"Camera License Key"** means an electronic key that will permit each license of Vigilant's CarDetector brand LPR software or LineUp brand facial recognition software (one CLK per camera) to be used with other Vigilant LPR hardware components and Software Products.

"Commercial LPR Data" refers to LPR data collected by private sources and available on LEARN with a paid subscription.

"Effective Date" means sixty (60) days subsequent to the date set forth in the first paragraph of this Agreement.

"Enterprise License" means a non-exclusive, non-transferable license to install and operate the Software Products, on any applicable media, without quantity or limitation. This Enterprise Service Agreement allows Affiliate to install the Software Products on an unlimited number of devices, in accordance with the selected Service Package(s), and allow benefits of all rights granted hereunder this Agreement.

"LEA LPR Data" refers to LPR data collected by LEAs and available on LEARN for use by other LEAs. LEA LPR Data is freely available to LEAs at no cost and is governed by the contributing LEA's retention policy.

"Service Fee" means the amount due from Affiliate prior to the renewal of this Agreement as consideration for the continued use of the Software Products and Service Package benefits according to Section VIII of this Agreement.

"Service Package" means the Affiliate designated service option(s) which defines the extent of use of the Software Products, in conjunction with any service and/or benefits therein granted as rights hereunder this Agreement.

BQ
VS Initials

Affiliate Initials

"Service Period" has the meaning set forth in Section III (A) of this Agreement.

"Software Products" means Vigilant's Law Enforcement & Security suite of Software Products including CarDetector, Law Enforcement Archival & Reporting Network (LEARN), Mobile Companion for Smartphones, Target Alert Service (TAS) server/client alerting package, FaceSearch, LineUp and other software applications considered by Vigilant to be applicable for the benefit of law enforcement and security practices.

"Technical Support Agents" means Affiliate's staff person specified in the Contact Information Worksheet of this Agreement responsible for administering the Software Products and acting as Affiliate's Software Products support contact.

"User License" means a non-exclusive, non-transferable license to install and operate the Software Products, on any applicable media, limited to a single licensee.

"Users" refers to individuals who are agents and/or sworn officers of the Affiliate and who are authorized by the Affiliate to access LEARN on behalf of Affiliate through login credentials provided by Affiliate.

II. Enterprise License Grant; Duplication and Distribution Rights:

Subject to the terms and conditions of this Agreement, Vigilant hereby grants Affiliate an Enterprise License to the Software Products for the Term provided in Section III below. Except as expressly permitted by this Agreement, Affiliate or any third party acting on behalf of Affiliate shall not copy, modify, distribute, loan, lease, resell, sublicense or otherwise transfer any right in the Software Products. Except as expressly permitted by this Agreement, no other rights are granted by implication, estoppels or otherwise. Affiliate shall not eliminate, bypass, or in any way alter the copyright screen (also known as the "splash" screen) that may appear when Software Products are first started on any computer. Any use or redistribution of Software Products in a manner not explicitly stated in this Agreement, or not agreed to in writing by Vigilant, is strictly prohibited.

III. Term; Termination.

A. Term. The initial term of this Agreement is for one (1) year beginning on the Effective Date (the "Initial Term"), unless earlier terminated as provided herein. Sixty (60) days prior to the expiration of the Initial Term and each subsequent Service Period, Vigilant will provide Affiliate with an invoice for the Service Fee due for the subsequent twelve (12) month period (each such period, a "Service Period"). This Agreement and the Enterprise License granted under this Agreement will be extended for a Service Period upon Affiliate's payment of that Service Period's Service Fee, which is due 30 days prior to the expiration of the Initial Term or the existing Service Period, as the case may be. Pursuant to Section VIII below, Affiliate may also pay in advance for more than one Service Period.

B. Affiliate Termination. Affiliate may terminate this Agreement at any time by notifying Vigilant of the termination in writing thirty (30) days prior to the termination date, and deleting all copies of the Software Products. If Affiliate terminates this Agreement prior to the end of the Initial Term, Vigilant will not refund or prorate any license fees, nor will it reduce or waive any license fees still owed to Vigilant by Affiliate. Upon termination of the Enterprise License, Affiliate shall immediately cease any further use of Software Products. Affiliate may also terminate this agreement by not paying an invoice for a subsequent year's Service Fee within sixty (60) days of invoice issue date.

C. Vigilant Termination. Vigilant has the right to terminate this Agreement by providing thirty (30) days written notice to Affiliate. If Vigilant's termination notice is based on an alleged breach by Affiliate, then Affiliate shall have thirty (30) days from the date of its receipt of Vigilant's notice of termination, which shall set forth in detail Affiliate's purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from Vigilant Affiliate has not reasonably cured the described breach of this Agreement, Affiliate shall immediately discontinue all use of Software Products and certify to Vigilant that it has returned or destroyed all copies of Software Products in its possession or control. If Vigilant terminates this Agreement prior to the end of a Service Period for no reason, and not based on Affiliate's failure to cure the breach of a material term or condition of this Agreement, Vigilant shall refund to Affiliate an amount calculated by multiplying the total amount of Service Fees paid by Affiliate for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365.

IV. Warranty and Disclaimer; Infringement Protection; Use of Software Products Interface.

A. Warranty and Disclaimer. Vigilant warrants that the Software Products will be free from all Significant Defects (as defined below) during the lesser of the term of this Agreement (the "Warranty Period") or one year. "Significant Defect" means a defect in a Software Product that impedes the primary function of the Software Product. This warranty does not include products not manufactured by Vigilant. Vigilant will repair or replace any Software Product with a Significant Defect during the Warranty Period; *provided, however*, if Vigilant cannot substantially correct a Significant Defect in a commercially reasonable manner, Affiliate may terminate this Agreement and Vigilant shall refund to Affiliate an amount calculated by multiplying the total amount of Service Fees paid by Affiliate for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365. The foregoing remedies are Affiliate's exclusive remedy for defects in the Software Product. Vigilant shall not be responsible for labor charges for removal or reinstallation of defective software, charges for transportation, shipping or handling loss, unless such charges are due to Vigilant's gross negligence or intentional misconduct. Vigilant disclaims all warranties, expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose. In no event shall Vigilant be liable for any damages whatsoever arising out of the use of, or inability to use, the Software Products.

B. Infringement Protection. If an infringement claim is made against Affiliate by a third-party in a court of competent jurisdiction regarding Affiliate's use of any of the Software Products, Vigilant shall indemnify Affiliate, and assume all legal responsibility and costs to contest any such claim. If Affiliate's use of any portion of the Software Products or documentation provided to Affiliate by Vigilant in connection with the Software Products is enjoined by a court of competent jurisdiction, Vigilant shall do one of the following at its option and expense within sixty (60) days of such enjoinment: (1) Procure for Affiliate the right to use such infringing portion; (2) replace such infringing portion with a non-infringing portion providing equivalent functionality; or (3) modify the infringing portion so as to eliminate the infringement while providing equivalent functionality.

C. Use of Software Products Interface. Under certain circumstances, it may be dangerous to operate a moving vehicle while attempting to operate a touch screen or laptop screen and any of their applications. It is agreed by Affiliate that Affiliate's users will be instructed to only utilize the interface to the Software Products at times when it is safe to do so. Vigilant is not liable for any accident caused by a result of distraction such as from viewing the screen while operating a moving vehicle.

V. Software Support, Warranty and Maintenance.

Affiliate will receive technical support by submitting a support ticket to Vigilant's company support website or by sending an email to Vigilant's support team. Updates, patches and bug fixes of the Software Products will be made available to Affiliate at no additional charge, although charges may be assessed if the Software Product is requested to be delivered on physical media. Vigilant will provide Software Products support to Affiliate's Technical Support Agents through e-mail, fax and telephone.

VI. Camera License Keys (CLKs).

Affiliate is entitled to use of the Software Products during the term of this Agreement to set up and install the Software Products on an unlimited number of media centers within Affiliate's agency in accordance with selected Service Options. As Affiliate installs additional units of the Software Products and connects them to LPR cameras, Affiliate is required to obtain a Camera License Key (CLK) for each camera installed and considered in active service. A CLK can be obtained by Affiliate by going to Vigilant's company support website and completing the online request form to Vigilant technical support staff. Within two (2) business days of Affiliate's application for a CLK, Affiliate's Technical Support Agent will receive the requested CLK that is set to expire on the last day of the Initial Term or the then-current Service Period, as the case may be.

VII. Ownership of Software.

A. Ownership of Software Products. The Software Products are copyrighted by Vigilant Solutions and remain the property of Vigilant Solutions. The license granted under this Agreement is not a sale of the Software Products or any copy. Affiliate owns the physical media on which the Software Products are installed, but Vigilant Solutions retains title and ownership of the Software Products and all other materials included as part of the Software Products.

B. Rights in Software Products. Vigilant Solutions represents and warrants that: (1) it has title to the Software and the authority to grant license to use the Software Products; (2) it has the corporate power and authority and the legal right to grant the licenses contemplated by this Agreement; and (3) it has not and will not enter into agreements and will not take or fail to take action that causes its legal right or ability to grant such licenses to be restricted.

VIII. Data Sharing, Access and Security.

If Affiliate is a generator as well as a consumer of LPR Data, Affiliate at its option may share its LEA LPR Data with similarly situated LEAs who contract with Vigilant to access LEARN (for example, LEAs who share LEA LPR Data with other LEAs). Vigilant will not share any LEA LPR Data generated by the Affiliate without the permission of the Affiliate.

Due to the growing concerns within the public safety sector surrounding aggregated LPR data, strict access to the LEARN data servers is required. To address this challenge, implementation of sophisticated hardware/software based intrusion protection has been deployed within the LEARN data center under the strict guidelines set forth by the National Security Association (NSA). The hosting facility utilizes state-of-the-art access control technologies. In addition, Vigilant has installed and configured a solid network intrusion prevention appliance provided by Cisco Systems Inc., as well as ensured that the configuration of the Microsoft environment adhere to the Windows Server 2008 Security Guide developed in conjunction with NSA to establish best practices. The net result is reduced risk (on all levels) of malicious

BQ
VS Initials

Affiliate Initials

intrusion and misuse. The network is secured by a Cisco 1812/K9 router that provides professional grade protection to the peripherals on the network. Amongst others, the Cisco IOS firewall firmware is compliant with PCI, HIPAA, and SOX IT governance requirements. The Cisco IOS firmware is also configured with Intrusion Protection Services that offers deep packet inspection on all incoming traffic.

IX. Ownership of LPR Data.

Vigilant retains all title and rights to Commercial LPR Data. Affiliate retains all rights to LEA LPR Data generated by the Affiliate. Should Affiliate terminate agreement with Vigilant, a copy of all LEA LPR Data generated by the Affiliate will be created and provided to the Affiliate. After the copy is created, all LEA LPR Data generated by the Affiliate will be deleted from LEARN at the written request of an authorized representative of the Affiliate.

X. Loss of Data, Irregularities and Recovery.

Vigilant places imperative priority on supporting and maintaining data center integrity. Using redundant disk arrays, there is a virtual guarantee that any hard disk failure will not result in the corruption or loss of the valuable LPR data that is essential to the LEARN system and clients.

XI. Data Retention and Redundancy.

LEA LPR Data is governed by the contributing LEA's retention policy. LEA LPR Data that reaches its expiration date will be deleted from LEARN. Vigilant's use of redundant power sources, fiber connectivity and disk arrays ensure no less than 99% uptime of the LEARN LPR database server system.

XII. Account Access.

A. Eligibility. Affiliate shall only authorize individuals who satisfy the eligibility requirements of "Users" to access LEARN. Vigilant in its sole discretion may deny access to LEARN to any individual based on such person's failure to satisfy such eligibility requirements. User logins are restricted to agents and sworn officers of the Affiliate. No User logins may be provided to agents or officers of other local, state, or Federal LEAs without the express written consent of Vigilant.

B. Security. Affiliate shall be responsible for assigning an Agency Manager who in turn will be responsible for assigning to each of Affiliate's Users a username and password (one per user account). A limited number of User accounts is provided. Affiliate will cause the Users to maintain username and password credentials confidential and will prevent use of such username and password credentials by any unauthorized person(s). Affiliate shall notify Vigilant immediately if Affiliate believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Affiliate must notify Vigilant immediately if Affiliate becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

XIII. Service Package, Fees and Payment Provisions.

A. Service Package. This Enterprise License Agreement is based on one (1) of the three (3) following Service Package Options. Please select one (1) Service Package below:

□ Service Package - Basic LPR Service Package:

- Vigilant Managed/Hosted LPR server LEARN Account
- Access to all Vigilant Software including all upgrades and updates
- Unlimited user licensing for the following applications:
  - LEARN, CarDetector and TAS

□ Service Package - Option # 1 – Standard LPR Service Package:

- All Basic Service Package benefits
- Unlimited use of CarDetector – Mobile Hit Hunter (CDMS-MHH)
- Unlimited use of Vigilant's LPR Mobile Companion smartphone application

□ Service Package - Option # 2 – 'Intelligence-Led Policing (ILP)' Service Package:

- All Service Package Option # 1 benefits
- Mobile or Fixed LPR hardware up to level of Tier (choice of either fixed or mobile packages, details in Exhibit A)
  - □ Reaper Cameras
  - □ Raptor 3 Cameras
- Use of Vigilant Facial Recognition technologies up to level of Tier
  - FaceSearch Account
  - FaceSearch Mobile Companion
  - Templates up to limit for FaceSearch Account (details in Exhibit A)
- Tiered based on size of department (Tier 1 up to 100 sworn officers, Tier 2 up to 200 sworn officers, Tier 3 up to 700 sworn officers, Tier 4 up to 2,000 sworn officers as well as Fusion Centers)
- States, Federal Agencies and Departments with greater than 2,000 sworn fall under a, "Custom" Tier which will be defined in the Annual Service Fee Schedule if applicable.

B. Service Fee. Payment of each Service Fee entitles Affiliate to all rights granted under this Agreement, including without limitation, use of the Software Products for the relevant Service Period, replacement of CLKs, and access to the updates and releases of the Software Products and associated equipment driver software to allow the Software Products to remain current and enable the best possible performance. The annual Service Fee due for a particular Service Period is based on the number of current Vigilant issued CLK's at the time of Service Fee invoicing, and which will be used by Affiliate in the upcoming Service Period. A schedule of annual Service Fees is shown below:

Annual Service Fee Schedule (multiplied by number of CLK's Issued)

Total # of CLK's under this ESA	0-14 CLK's	15-30 CLK's	31-60 CLK's	Over 60
Basic Service	$525.00	$450.00	$400.00	$275.00
Standard (Option # 1)	$750.00	$640.00	$565.00	$390.00
ILP Subscriber CLK Renewal Fees	$525.00	$450.00	$400.00	$275.00

BQ
VS Initials

Affiliate Initials

Annual Service Fee Schedule for Intelligence-Led Policing (ILP) Service Package

Tier	Reaper	Raptor 3
ILP Tier 1 (Option # 2)	$14,995.00	$14,995.00
ILP Tier 2 (Option # 2)	$34,495.00	$34,495.00
ILP Tier 3 (Option # 2)	$89,495.00	$89,495.00
ILP Tier 4 (Option #2)	$154,495.00	$154,495.00

Annual Service Fee Schedule for Image Enrollment (applicable to FaceSearch/LineUp images only)

5,000 Images	$750.00

Payment of the Service Fee is due thirty (30) days prior to the renewal of the then-current Service Period. All Service Fees are exclusive of any sales, use, value-added or other federal, state or local taxes (excluding taxes based on Vigilant's net income) and Affiliate agrees to pay any such tax. Service Fees may increase by no higher than 4% per year for years after the first year of this agreement. For ILP (Option # 2) Tier packages, the Tier amount is due for subsequent periods and Basic Service CLK fees are due for all cameras from previous periods (this is in addition to the Annual Subscription Fee).

C. Advanced Service Fee Payments. Vigilant Solutions will accept advanced Service Fee payments on a case by case basis for Affiliates who wish to lock in the Service Fee rates for subsequent periods at the rates currently in effect, as listed in the table above. If Affiliate makes advanced Service Fee payments to Vigilant Solutions, advanced payments to Vigilant Solutions will be applied in full to each subsequent Service Period's Service Fees until the balance of the credits is reduced to a zero balance. System based advanced credits shall be applied to subsequent Service Fees in the amount that entitles Affiliate continued operation of the designated camera unit systems for the following Service Period until the credits are reduced to a zero balance.

D. Price Adjustment. Vigilant has the right to increase or decrease the annual Service Fee from one Service Period to another; *provided, however*, that in no event will a Service Fee be increased by more than the greater of (i) 4% of the prior Service Period's Service Fees, (ii) the published rate of inflation in the United States for the prior year then ended, or (iii) prices identified in the original proposal. If Vigilant intends to adjust the Service Fee for a subsequent Service Period, it must give Affiliate notice of the proposed increase on or before the date that Vigilant invoices Affiliate for the upcoming Service Period.

XIV. Miscellaneous.

A. Limitation of Liability. IN NO EVENT SHALL VIGILANT SOLUTIONS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES INCLUDING DAMAGES FOR LOSS OF USE, DATA OR PROFIT, ARISING OUT OF OR CONNECTED WITH THE USE OF THE SOFTWARE PRODUCTS, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF VIGILANT SOLUTIONS HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IN NO EVENT WILL VIGILANT SOLUTIONS'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE FEES PAID BY AFFILIATE TO VIGILANT SOLUTIONS FOR THE SOFTWARE PRODUCTS LICENSED UNDER THIS AGREEMENT.

B. Confidentiality. Affiliate acknowledges that Software Products contain valuable and proprietary information of Vigilant Solutions and Affiliate will not disassemble, decompile or reverse engineer any Software Products to gain access to confidential information of Vigilant Solutions.

C. Assignment. Neither Vigilant Solutions nor Affiliate is permitted to assign this Agreement without the prior written consent of the other party. Any attempted assignment without written consent is void.

D. Amendment; Choice of Law. No amendment or modification of this Agreement shall be effective unless in writing and signed by authorized representatives of the parties. This Agreement shall be governed by the laws of the state of California without regard to its conflicts of law.

E. Complete Agreement. This Agreement constitutes the final and complete agreement between the parties with respect to the subject matter hereof, and supersedes any prior or contemporaneous agreements, written or oral, with respect to such subject matter.

F. Relationship. The relationship created hereby is that of contractor and customer and of licensor and Affiliate. Nothing herein shall be construed to create a partnership, joint venture, or agency relationship between the parties hereto. Neither party shall have any authority to enter into agreements of any kind on behalf of the other and shall have no power or authority to bind or obligate the other in any manner to any third party. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Each party hereto represents that it is acting on its own behalf and is not acting as an agent for or on behalf of any third party.

G. No Rights in Third Parties. This agreement is entered into for the sole benefit of Vigilant Solutions and Affiliate and their permitted successors, executors, representatives, administrators and assigns. Nothing in this Agreement shall be construed as giving any benefits, rights, remedies or claims to any other person, firm, corporation or other entity, including, without limitation, the general public or any member thereof, or to authorize anyone not a party to this Agreement to maintain a suit for personal injuries, property damage, or any other relief in law or equity in connection with this Agreement.

H. Construction. The headings used in this Agreement are for convenience and ease of reference only, and do not define, limit, augment, or describe the scope, content or intent of this Agreement. Any term referencing time, days or period for performance shall be deemed calendar days and not business days, unless otherwise expressly provided herein.

I. Severability. If any provision of this Agreement shall for any reason be held to be invalid, illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this Agreement, such provision shall be construed so as to make it enforceable to the greatest extent permitted, such provision shall remain in effect to the greatest extent permitted and the remaining provisions of this Agreement shall remain in full force and effect.

J. Federal Government. Any use, copy or disclosure of Software Products by the U.S. Government is subject to restrictions as set forth in this Agreement and as provided by DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227 (ALT III), as applicable.

K. Right to Audit. Affiliate, upon thirty (30) days advanced written request to Vigilant Solutions, shall have the right to investigate, examine, and audit any and all necessary non-financial books, papers, documents, records and personnel that pertain to this Agreement and any other Sub Agreements.

L. Notices; Authorized Representatives; Technical Support Agents. All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person; (b) sent by facsimile transmission indicating receipt at the facsimile number where sent; (c) one (1) business day after being deposited with a reputable overnight air courier service; or (d) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. All notices and communications regarding default or termination of this Agreement shall be delivered by hand or sent by certified mail, postage pre-paid and return receipt requested. Either party may from time to time change the notice address set forth below by delivering 30 days advance notice to the other party in accordance with this section setting forth the new address and the date on which it will become effective.

Vigilant Solutions, LLC	**Affiliate:** AZDPS
Attn: Sales Administration	Attn: Criminal Investigations
2021 Las Positas Court - Suite # 101	Address: 2102 W Encanto Blvd
Livermore, CA 94551	Phoenix, AZ 85009

M. Authorized Representatives; Technical Support Agents. Affiliate's Authorized Representatives and its Technical Support Agents are set forth below (Last Page). Affiliate's Authorized Representative is responsible for administering this Agreement and Affiliate's Technical Support Agents are responsible for administering the Software Products and acting as Affiliate's Software Products support contact. Either party may from time to time change its Authorized Representative, and Affiliate may from time to time change its Technical Support Agents, in each case, by delivering 30 days advance notice to the other party in accordance with the notice provisions of this Agreement.

BQ
VS Initials

Affiliate Initials

IN WITNESS WHEREOF, the parties have executed the Agreement as of the Effective Date.

Manufacturer: Vigilant Solutions, LLC

Authorized Agent: Bill Quinlan

Title: Director, Global Sales Operations

Date: 11-1-2016

Signature:

Affiliate Organization: Arizona DPS

Authorized Agent: Colonel Frank Milstead

Title: Director

Date: 10.13.16

Signature:

VIGILANT
SOLUTIONS

Enterprise Service Agreement

Contact Information Worksheet

Please complete the following contact information for your Vigilant Solutions Enterprise License program.

Enterprise License Agreement Holder			
Company / Agency Name:			
Company / Agency Type:			
Address:			
Primary Contact			
Name:			
Title:		Phone:	
Email:			
Supervisor Information			
Name:			
Title:		Phone:	
Email:			
Financial Contact (Accounts Payable)			
Name:			
Title:		Phone:	
Email:			
Technical Support Contact # 1			
Name:			
Title:		Phone:	
Email:			
Technical Support Contact # 2			
Name:			
Title:		Phone:	
Email:			

For questions or concerns, please contact Vigilant Solutions' sales team:

sales@vigilantsolutions.com

1-925-398-2079

Exhibit A: Option # 2 ILP Tier Package Components

Part #	Item Description
VS-ILP-1M2RE / VS-ILP-1M2R3	**ILP Mobile Bundle for Agencies of Up to 100 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - One (1) 3-camera mobile LPR system - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 5,000 images
VS-ILP-1F2RE / VS-ILP-1F2R3	**ILP Fixed Bundle for Agencies of Up to 100 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Three (3) fixed camera LPR systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 5,000 images
VS-ILP-2M2RE / VS-ILP-2M2R3	**ILP Mobile Bundle for Agencies of 51 to 200 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Two (2) 3-camera mobile LPR system - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 20,000 images
VS-ILP-2F2RE / VS-ILP-2F2R3	**ILP Fixed Bundle for Agencies of 51 to 200 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Six (6) fixed camera LPR systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 20,000 images

VS-ILP-3M2RE / VS-ILP-3M2R3	**ILP Mobile Bundle for Agencies of 201 to 700 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Four (4) 3-camera mobile LPR system - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 50,000 images
VS-ILP-3F2RE / VS-ILP-3F2R3	**ILP Fixed Bundle for Agencies of 201 to 700 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Twelve (12) fixed camera LPR systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 50,000 images
VS-ILP-4M2RE / VS-ILP-4M2R3	**ILP Mobile Bundle for Fusion Centers and Agencies of 701 to 2000 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Five (5) 3-camera mobile LPR system - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 100,000 images
VS-ILP-4F2RE / VS-ILP-4F2R3	**ILP Fixed Bundle for Fusion Centers and Agencies of 701 to 2000 Sworn** Includes: - Agency license for LEARN SaaS - Unlimited access to Commercial LPR data - Fifteen (15) fixed camera LPR systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 100,000 images

VIGILANT
SOLUTIONS

LEARN-NVLS

National LPR Database

Security Document

Managed / Hosted Solution

For Law Enforcement Use Only

Preface:

Vigilant Solutions Incorporated (Vigilant) is a technology company that specializes in providing advanced video content analysis algorithms and data distribution networks. As the use of License Plate Recognition (LPR) technology has grown within the United States, this technology has proven itself to be an invaluable asset to law enforcement. Due to the rapid proliferation of this technology, a strong and growing need exists to share LPR scan data between law enforcement agencies. Specifically for this reason, Vigilant has developed an answer to that need – LEARN-NVLS.

The LEARN-NVLS database server is the key component that makes LPR data sharing possible for the typical Law Enforcement Agency (LEA). LEARN-NVLS allows for LEA access to the United States' largest LPR database wherein as of October 2013 over 1.4 billion vehicle location data records reside with a continued addition of 60-80 million new LPR data records each month. This server remains protected from the public and requires a bona fide LEA and/or valid ORI code for access.

Vigilant offers a hosted and managed LPR data center solution to all of its LEA LPR technology customers via the LEARN-NVLS LPR database server. This includes access and use to its Law Enforcement Archival Reporting Network (LEARN) LPR server application. The LEARN-NVLS server has quickly established a national footprint of top tier LEA users. The public safety impact of LEARN-NVLS uniting LEAs across the country within a common LPR data sharing framework should not be underestimated.

Within the context of maintaining a centrally managed server to house valuable law enforcement data in conjunction with protecting the public from those that choose to do harm unto others, it is imperative the highest measures of security and reliability are implemented. This document outlines the measures taken and infrastructure established to ensure that LEA customers have a highly secure and reliable data hosting option for their LPR system management and storage. Through the trusted guarantees of the hosting provider, Verio (an NTT Communications Company), and the trend setting standards of Cisco Systems Inc., the integrity and security of the LEARN-NVLS National LPR Database server system are assured.

The aim of this document is to describe various aspects of the Vigilant National LEARN-NVLS LPR database server in the hopes that your understanding and involvement will accelerate the value of this endeavor to the LEA community.

About our Hosting Partner:

Verio has been chosen to host the LEARN-NVLS server for many reasons, not least of which it is chosen by many unnamed Federal and Fortune 500 companies. Their commitment to reliability is exceptional and their facilities are state-of-the-art, providing the perfect environment to house the LEARN-NVLS server system.

Verio is the recognized industry leader in delivering online business solutions to SMBs worldwide. Distributed through its network of OEM channel partners, Verio's solutions provide web hosting, application hosting and Software-as-a-Service (SaaS) applications that enable SMBs to drive online success.

Incorporated in 1996, the company launched a successful public offering in 1998. This IPO set the stage for a series of acquisitions of rapidly growing hosting and Internet companies which resulted in Verio emerging as the preeminent provider of web hosting services worldwide. In 2000, the company became a wholly owned subsidiary of NTT Communications, one of the largest companies in the world and supports its operations through NTTs highly reliable and scalable Global IP Network. Through this network, customers and partners can extend their global reach with access to business solutions around the globe and in more than 200 countries.

Today, Verio leverages its financial strength and stability to support its growing customer base, extend its product leadership and expand its global footprint for partners worldwide.

World Class Support Staff:

The LEARN-NVLS onsite professional technical, support, and engineering team maintain numerous certifications to ensure up to date compliance and familiarity with the latest standards in computer technology. These certifications include:

- Certified Information System Security Professional (CISSP)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Internetwork Expert (CCIE)
- Cisco Certified Design Professional (CCDP)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Design Associate (CCDA)
- CompTIA A+, CompTIA i-Net+, CompTIA Security+
- Sun Certified System Administrator (SCSA)
- Microsoft Certified Systems Administrator (MCSA)
- Alteon Certified Administrator
- Solaris 8 System Administrator
- Microsoft Certified Systems Engineer (MCSE)
- Red Hat Certified Engineer (RHCE)
- Microsoft Certified Professional (MCP)

Data Facility Accreditations:

There are numerous accreditations that qualify the LEARN-NVLS data server facility and demonstrate Vigilant's commitment to providing a top-tier hosting facility. Verio is a Microsoft Gold Certified Partner, providing a high level of quality assurance with all hosted Microsoft products. Verio is certified ISO 9001:2008, the internationally recognized standard for Quality Management Systems, and has been independently audited and verified for compliance under the Statement of Auditing Standards Number 70 [SAS70] Type II.

To maintain leadership and renown in the industry, the data center hosting company remains affiliated with and participates in the IEC [International Engineering Consortium], ASNP [Association of Storage Networking Professionals], CSI [Computer Security Institute], IEEE [Institute of Electrical and Electronics Engineers, Inc.], CompTIA [The Computing Technology Industry Association], IETF [Internet Engineering Task Force], and the ASTD [American Society for Training and Development].

Data Facility Features:

The premier LEARN-NVLS data centers features:

- Redundant Power Sources
- Redundant Fiber Connectivity
- OC12 & OC48 Connectivity
- HVAC Environmental Monitoring
- Secure Physical Access Control
- Physical Escort for Onsite Visitors
- Multiple Diesel Fuel Generators
- Active Fire Prevention & Suppression
- 24 X 7 Monitoring and Operational Support
- Onsite System Administrators/Engineers

The LEARN-NVLS datacenter facility physically residing in the state of Virginia is strategically located within immediate response of Verio's top facilities support staff headquartered in Washington DC, one of the most security-conscious regions of the country. Vigilant selected this location to further enhance its commitment of providing peace of mind and stability to end user LEA customers, making Verio the perfect fit for hosting the LEARN-NVLS server system.

Data Center:

With years of experience in managing thousands of LPR cameras connected to a single data server, Vigilant has taken great care to develop a data distribution architecture required for centralized data repository success. The data being stored and the interfaces offered via LEARN-NVLS prove great value to LEAs nationwide. To date the LEARN-NVLS design (and commercially available use) has proven unmatched to overcoming the challenges inherent to advanced LPR technology. This is largely due to the system's versatility and ease of user integration.

The layout of the LEARN-NVLS data center is unique in that it embraces the strengths of application distribution and load decentralization to allow for the work of LEARN-NVLS to be split across multiple servers. The software is designed to be extensible between many coordinating servers making LEARN-NVLS scalable to accommodate an infinite number of users. The server hardware architecture and components have been selected to ensure redundancy. Each of these attributes are woven to form a safe, secure, and reliable LPR data center with minimal hardware failure, system downtime, and data storage risk.

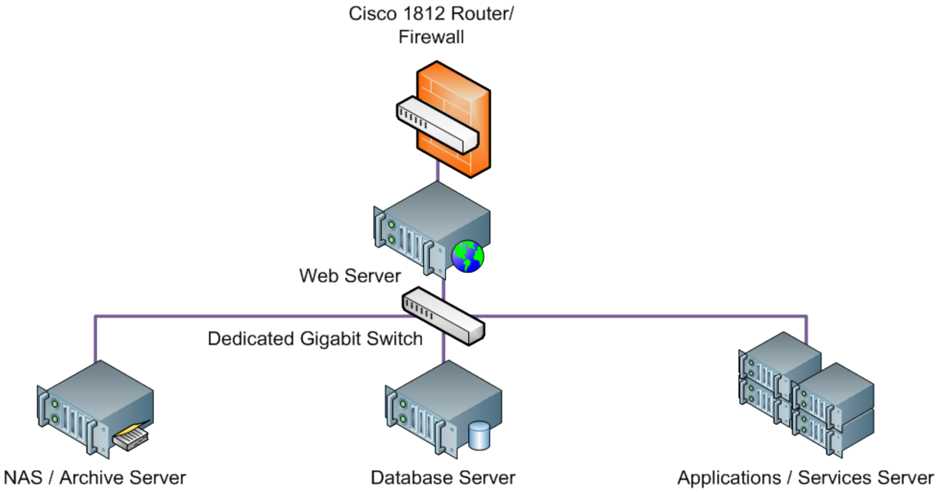
Scalability

The LEARN-NVLS system was created with scalability as a top priority. With performance measures and rigorous testing, the LEARN-NVLS software is capable of scaling in excess of 100,000 LPR cameras with 50,000 simultaneous user connections. Using stateless web sessions, dedicated services for intra-system disk tasks, Microsoft Message Queue [MSMQ] for intra-system communication, and the powerful MS SQL

Server database for records management, the LEARN-NVLS LPR data server is engineered to efficiently meet the expectations of a rapidly expanding user base with minimal production changes. Currently, the LEARN-NVLS system is distributed across 4 servers:

- Web Server
- Applications Server
- Database Server
- NAS Archive Server

The system architecture is as follows:



With the web server managing the end user interfaces, the database server managing the data, the applications server managing the communication between the file systems and message queues, and the archive server managing the redundant backups, the system functions smoothly and efficiently for the current user base.

As the LEARN-NVLS enterprise system grows, servers may readily be added to support an increasing number of users and LPR peripherals. Adding web server(s) with round-robin load-balancing routers provides additional resources allocated to manage countless concurrent connections. Additional application servers may be dedicated to resource-intensive tasks therefore maintaining user expected performance. The flexibility of SQL Server allows a myriad of solutions addressing improved system performance - including dedicated SAN's, RAM drives for high traffic tables, and database clustering for load distribution.

With such distributable architecture, Vigilant's LPR clients are guaranteed LEARN-NVLS enterprise system use to remain scalable and flexible as the market demands of LPR technology grows. These services are offered to all Vigilant LEA clients that elect to utilize the LEARN-NVLS managed / hosted solution.

Security:

Due to the growing concerns within the public safety sector surrounding aggregated LPR data, strict access to the LEARN-NVLS data servers is not only required but commanded. To address this challenge, implementation of sophisticated hardware/software based intrusion protection has been deployed within the LEARN-NVLS data center under the strict guidelines set forth by the National Security Association (NSA).

While Verio provides the physical security, Vigilant has installed and configured a solid network intrusion prevention appliance provided by Cisco Systems Inc., as well as ensured that the configuration of the Microsoft systems meet the strict guidelines requisite of a top tier law enforcement system. The net result is reduced risk (on all levels) of malicious intrusion and misuse.

The network is secured by a Cisco 1812/K9 router that provides professional grade protection to the peripherals on the network. Amongst others, the Cisco IOS firewall firmware is compliant with PCI, HIPAA, and SOX IT governance requirements. The Cisco IOS firmware is also configured with Intrusion Protection Services that offers deep packet inspection on all incoming traffic. For more information, resources can be found at: www.cisco.com

The Windows environment has been built to adhere to the Windows Server 2003 Security Guide developed in conjunction with the NSA to establish best practices. The NSA website states:

> *The Special Security - Limited Functionality (SSLF) settings in Microsoft's Windows Server 2003 Security Guide track closely with the security level historically represented in the NSA guidelines. It is our belief that this guide establishes the latest best practices for securing the product and recommend that traditional customers of our security recommendations use the Microsoft guide when securing Windows Server 2003.*

http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems/microsoft_windows.shtml

With security and safety at the forefront of Vigilant's concerns in establishing and supporting a National LPR Initiative, leading edge systems and industry tested configurations have been employed to create an environment fit to support state-of-the-art License Plate Recognition Enterprise Server, LEARN, dedicated to the exclusive use of law enforcement.

Additionally, an auditing system has been implemented to trace at every level of data interaction. Should the event of misuse occur within the system, LEAs are assured all activity can be traced to a time, place, and source location.

Reliability:

Vigilant places imperative priority on supporting and maintaining data center integrity. Employing Verio's hosting standards for redundancy and wide failover safeguards ensure minimum system downtime. Using redundant disk arrays, there is a virtual guarantee that any hard disk failure will not result in the corruption or loss of the valuable LPR data that is essential to the LEARN-NVLS system and clients. Coupled with redundant power supplies and 24x7 emergency support by Vigilant, the LEARN-NVLS LPR database server system guarantees no less than 99% uptime of the LEARN and NVLS website applications.

Disclaimer: Verio, via Verio and the Verio logo are registered trademarks and/or service marks of Verio Inc. in the United States and other countries. All other names are trademarks or registered marks of their respective owners. References provided by http://www.verio.com.

Summary of Points Covered

The LEARN-NVLS National LPR Data Repository is a safe and secure solution for hosting Law Enforcement Agency LPR data for many reasons. Some of the following points below highlight the credibility and security measures taken by Vigilant to ensure the success of the LEARN-NVLS LPR data hosting program for Law Enforcement Agencies only:

- The LEARN-NVLS data center is located in the state of Virginia
- Verio is the elected hosting company
- The data center is certified SAS70 Type II and ISO9001:2008
- Data server access is limited to Verio, Vigilant, and qualifying ORI coded LEA customers
- Verified compliance under the Statement of Auditing Standards Number 70 [SAS70] Type II
- LEARN-NVLS LPR database server system guarantees no less than 99% uptime
- The network is secured by a Cisco 1812/K9 router
- LEARN-NVLS was designed for an excess of 100,000 LPR cameras / 50,000 simultaneous connections
- The LEARN-NVLS database stores over 430,000,000 records with 35,000,000 records added monthly
- The server offers redundant power supplies and 24x7 emergency support
- Redundant disk arrays offer a virtual guarantee against data loss or corruption
- Onsite System Administrators and Engineers - 24 X 7 Monitoring and Operational Support
- The Cisco IOS is configured with Intrusion Protection that offers deep packet inspection on all traffic
- Server configuration follows strict guidelines set forth by the National Security Association (NSA)

Please feel free to share this information with the other team members including any of the LEAs within your area. It is our hope that this paper has provided a quick and concise understanding of the system offered to law enforcement agencies across the United States, the Nation’s 1st LPR database repository.

Agency Manager
List Report

Name	Phone	Email
Damon Cecil	6022232629	dceciliii@azdps.gov
Mang Vinh	6022232854	mvinh@azdps.gov
STEVE JIMENEZ	602-223-2364	SJIMENEZ@AZDPS.GOV
JOHN MOURET	602-223-2364	JMOURET@AZDPS.GOV
DAVID CALLISTER	602-223-2364	DCALLISTER@AZDPS.GOV
Robert Huijkman	602-845-8326	rhuijkman@azdps.gov
Brandon Dyson	602-845-8326	bdyson@azdps.gov
Terry Dishroon	5207464683	TDishroon@azdps.gov
Tiffany Chung	-602-644-5773	TNChung@AZDPS.GOV
Paul Etnire	6022232015	petnire@azdps.gov

Detections Shared

The Arizona Department of Public Safety Agency is Sharing its Detection data with the following Agencies:

100th Judicial District Attorney Traffic Enforcement
17th Judicial Circuit Drug Task Force
21st Drug Task Force
24th Judicial District Drug Task Force
32nd Judicial District Attorney Office
Aberdeen Police Department
Alameda County Narcotics Task Force
Alameda Police Department
Alamo Heights TX PD
Alamosa County Sheriffs Department
Allen Police Department
Anaheim Police Department
Antioch Police Department CA
Arcadia Police Department
Arlington Police Department (TX)
Auburn Police Department
Austin Police Department
Austin Regional Intelligence Center
Bakersfield Police Department
Baldwin County Sheriffs Office
Beaumont Police Department TX
Bessemer Police Department
Beverly Hills Police Department
Binghamton Police Department
Birmingham Police Department
Blythe Police Department
Bolivar Police Department
Boone County Sheriff Office
Brea Police Department
Brentwood Police Department
Burbank Police Department
Burnet County TX Law Enforcement
Burr Ridge Police Department
Byron Police Department
Calumet City Police Department
Carlsbad Police Department
Carroll County Sheriffs Office
Carrollton Police Department
Carrollton Police Department TX
Carson City Sheriffs Dept
Casa Grande Police Department
Cathedral City Police Department
Cedar Rapids Police Department
Chicago HIDTA
Chicago Police Department
Chino Police Department
Chula Vista Police Department
Cincinnati Police Department
Clackamas County Sheriffs Office
Claremont Police Department
Clovis Police Department
College Park Police Department
College Station Police Department
Comer Police Department
Contra Costa County Sheriffs
Cook County States Attorney
Corona Police Department
Costa Mesa Police Department
County of San Mateo Sheriffs Office
Covington Police Department
Coweta County Sheriffs Office
Dallas Police Department

Danville Police Department CA

Daphne Police Department

Decatur Police Department

Deer Park Police Department

DeKalb County Police Department

Denton Police Department

DFW Airport

DHS - HSI - New Orleans

DHS Bulk Cash Smuggling Center

District 21 Drug Task Force

DOJ - Bureau of Firearms

Douglas County Sheriffs Office

Douglasville Police Department

Downey Police Department

Drug Task Force 17th Judicial District

Dublin Police Department

Dublin Police Department (OH)

Dublin Police Department CA

Duluth Police Department

Dutchess County Sheriff

East Chicago Police Department

Edinburg Police Department

El Cajon Police Department

El Paso Police Department

Elk Grove Police Department

Elk Grove Village Police Department

Fairfield Police Department CA

Fayette CO TX SO

Fayette County Sheriffs Office

Federal Bureau of Investigation

Folsom Police Department

Fontana Police Department

Fort Worth Police Department

Fountain Valley Police Department

Fresno Police Department

Fullerton Police Department

Galveston Auto Theft Task Force

Garden Grove Police Department

Gardena Police Department

Geary County Sheriff

Guadalupe County Constables

Guadalupe County Sheriffs Office

Gwinnett County Police Department

Hamilton County Sheriff (IN)

Hammond Police Department

Hawthorne Police Department

Hayward Police Department

Hickory Hills Police Department

HIDTA - Central Valley California

Hiram Police Department

Hollywood Park Police Department

Hollywood Police Department (Fl)

Hoover Police Department

Hopkinsville Police Department

Houston Police Department

Huntington Beach Police Department

Imperial County Regional ALPR Program

Indiana State Police

Indianapolis Division Homeland Security

Indianapolis Police Department

Irvine Police Department

Jackson County Sheriffs Office

Jasper County Sheriff MO

Jasper County Sheriffs Office MS

Jefferson CO TX SO

Jones County Sheriffs Department

Jonesboro Police Department

Joplin Police Department

Kansas City Police Department

Killeen Texas Police Department

L.A. County Sheriffs Dept

Lafayette Police Department (LA)

Laguna Beach Police Department

Lamar County Sheriffs Department

Lanier County Sheriffs Office

Las Vegas Metro Police Department

Lee County Sheriffs Office

Liberty County Sheriffs Office (TX)

Lincoln County Sheriff MO

Lithonia Police Department

Livermore Police Department

Lodi Police Department

Long Beach Police Department

Los Alamitos Police Department

Los Angeles County Sheriff

Lufkin Police Department

Lumber City Police Department

Manteca Police Department

Maricopa Police Department

Marin County Sheriffs Office

Medford Police Department

Merced Police Department CA

Meridian Police Department

Mesa Police Department

Mesquite Police Department

Mesquite Police Department (NV)

Midland Police Department

Milton Police Department

Modesto Police Department

Monroe County Sheriffs Office

Monrovia Police Department

Munster Police Department

Nevada Police Department

New York State Police

Newark Police Department New Jersey

Newport Beach Police Department

NW HIDTA - Seattle

Ogden Police Department

Ontario County Sheriffs Office

Ontario Police Department

Orange County Sheriff

Orange County Sheriff (TX)

Orange County Sheriffs Department

Orange Police Department TX

Oswego County Sheriffs Office

Oxnard Police Department

Palm Beach County Sheriffs

Pasadena Police Department (CA)

Pasadena Police Department (TX)

Pascagoula Police Department

Pearl Police Department

Phoenix Police Department

Pima County Sheriff

Pine Mountain Police Department

Pittsburg Police Department CA

Plano Police Department

Pleasanton Police Department

Poplar Bluff Police Department

Port of Long Beach

Putnam County Sheriff

Rankin County Sheriffs Office

Redlands Police Department

Redondo Beach Police Department

Reeve County Sherriffs Office

Reno Police Department

Richmond County Sheriffs Office

Riverdale Police Department

Riverside Police Department

Riverside Police Department (MO)

Rockwall County Sheriffs

Roswell Police Department

Round Rock PD

Sacramento County DA Office

Sacramento County Sheriffs Office

Sacramento Police Department

Sacramento Probations Department

San Bernardino County Sheriffs

San Bernardino Police Department

San Diego County Sheriff

San Diego Police Department

San Diego Regional Auto Theft Task Force

San Diego Sector Border Patrol

San Juan Police Department

San Luis Obispo Sheriffs Office

San Rafael Police Department

San Ramon Police Department

Santa Ana Police Department

Santa Clara Police Department

Santa Fe Police Department

Saraland Police Department

Schererville Police Department

Scottsdale Police Department

Seal Beach Police Department

Simi Valley Police Department

Solano County Sheriffs Department

South Carolina Law Enforcement Division

South Gate Police Department

South Pasadena Police Department

Sparks Police Department

Springfield IL Police Department

Springfield MO Police Department

Stanislaus County Auto Theft Task Force

Stockton Police Department

Sumter County Sheriffs Office

Tempe Police Department

Temple Police Department

Tennessee HLS District 7

Texas City Police Department

Texas Department of Public Safety

Torrance Police Department

Travis County SO

Trussville Police Department

Ulster County Sheriffs Office

United States Forest Service CA

United States Forest Service Utah

United States Marshals Service

Vancouver Police Department

Walnut Creek Police Department

Washoe County Sheriffs Office

Watauga Police Department

Webster Grove Police Dept

Webster Police Department

West Covina Police Department

West Sacramento Police Department

Whittier Police Department

Williamson County Sheriffs Office

Woodstock Police Department

Detections Received

The Arizona Department of Public Safety Agency is receiving Detection data from the following Agencies:

Coweta County Sheriffs Office
Riverside Police Department
Fort Worth Police Department
UC Irvine Police Department
Irvine Police Department
Novato Police Department
Pleasanton Police Department
Hiram Police Department
Lees Summit Police Department
Webster Police Department
Sacramento County Sheriffs Office
Elk Grove Police Department
Brentwood Police Department
Bakersfield Police Department
Allen Police Department
El Paso Police Department
Round Rock PD
Cathedral City Police Department
Douglas County Sheriffs Office
Lee County Sheriffs Office
College Park Police Department
Bessemer Police Department
Hopkinsville Police Department
Hickory Hills Police Department
Phoenix Police Department
Chino Police Department
Gwinnett County Police Department
Downers Grove Police Department
Fresno Police Department
Comer Police Department
Harris County Sheriffs Office
Byron Police Department
Anaheim Police Department
Athens-Clarke Police Department
Sacramento Police Department
Corona Police Department
Marin County Sheriffs Office
Joplin Police Department
Carrollton Police Department
Duluth Police Department
Reno Police Department
Webster Grove Police Dept
United States Forest Service CA
Dallas Police Department
Bronxville Police Department
San Bernardino County Sheriffs
Hoover Police Department
Fayette County Sheriffs Office
Jones County Sheriffs Department
Newark Police Department New Jersey
Austin Police Department
Milton Police Department
Travis County SO
Rockwall County Sheriffs
Binghamton Police Department
Pittsburg Police Department CA
DeKalb County Police Department
Roswell Police Department
Long Beach Police Department
Tulare Police Department

Woodstock Police Department

Schererville Police Department

Pascagoula Police Department

Lee County Alabama Sheriffs Office

Alameda Police Department

San Diego Regional Auto Theft Task Force

21st Drug Task Force

Baldwin County Sheriffs Office

17th Judicial Circuit Drug Task Force

East Chicago Police Department

Guadalupe County Sheriffs Office

New York State Police

Sacramento County DA Office

South Carolina Law Enforcement Division

Southwest Major Case Unit (IL)

Mundelein Police Department

County of San Mateo Sheriffs Office

Walnut Creek Police Department

Simi Valley Police Department

Orange County Sheriff (TX)

West Baton Rouge

Cedar Rapids Police Department

Calumet City Police Department

Solano County Sheriffs Department

Jasper County Sheriffs Office MS

South Gate Police Department

Torrance Police Department

Modesto Police Department

Lincoln County Sheriff MO

Downey Police Department

Jefferson CO TX SO

United States Marshals Service

Midland Police Department

Bartow County Sheriffs Office

Dickinson Police Department

San Luis Obispo Sheriffs Office

Lumber City Police Department

Rankin County Sheriffs Office

Chula Vista Police Department

Munster Police Department

College Station Police Department

Meridian Police Department

Pine Mountain Police Department

Guadalupe County Constables

Alameda County Narcotics Task Force

West Covina Police Department

HIDTA - Central Valley California

Monroe County Sheriffs Office

San Bernardino Police Department

Liberty County Sheriffs Office (TX)

Hamilton County Sheriff (IN)

Burr Ridge Police Department

Burnet County TX Law Enforcement

Geary County Sheriff

Oxnard Police Department

Fayette CO TX SO

Cook County States Attorney

Manteca Police Department

Palos Verdes Estates Police Department

Dublin Police Department (OH)

Bolivar Police Department

Danville Police Department CA

Nevada Police Department

Mesa Police Department

24th Judicial District Drug Task Force

Merced Police Department CA

Casa Grande Police Department

Monrovia Police Department

Trussville Police Department

Midlothian Police Department

Bell Police Department

Edinburg Police Department

Killeen Texas Police Department

Nacogdoches Police Department

Carlsbad Police Department

Carrollton Police Department TX

Saraland Police Department

Watauga Police Department

Daphne Police Department

Dutchess County Sheriff

Vancouver Police Department

Department of Transportation - Phoenix Arizona

Lafayette Police Department (LA)

Westport Police Department

Paradise Valley Police Department

Putnam County Sheriff

Pima County Sheriff

Boone County Sheriff Office

Reeve County Sherriffs Office

Ossining Police Department

Plainville Police Department

Stratford Police Department

Norwalk Police Department

Oklahoma Bureau of Narcotics

Oxford Police Department

Upland Police Department (CA)

Hammond Police Department

Douglasville Police Department

Hollywood Police Department (Fl)

Gardena Police Department

Ulster County Sheriffs Office

Redondo Beach Police Department

Missouri City Police Department

Conroe Police Department

32nd Judicial District Attorney Office

Poplar Bluff Police Department

Medford Police Department

Stockton Police Department

Williamson County Sheriffs Office

Imperial County Regional ALPR Program

District 21 Drug Task Force

Redlands Police Department

Foley Police Department

Junction City Police Department

DOJ - Bureau of Firearms

100th Judicial District Attorney Traffic Enforcement

Hendersonville Police Department

Maricopa Police Department

Commerce City Police Department

Enfield Police Department

Wethersfield Police Department

Trumbull Police Department

Union City Police Department (CA)

US Army CID

Westover Hills Police Department

Hot-List Sharing

The Arizona Department of Public Safety Agency is sharing Hot-List records with the following Agencies:

Agency: **Hot-List(s):**

None	None

Hot-List Received

The Arizona Department of Public Safety Agency is receiving Shared Hot-List records from the following Agencies:

Agency:	**Hot-List(s):**
Montgomery Police Department	HSI MASTER

LEARN

Accuracy

Dashboard Accuracy Report

VIGILANT SOLUTIONS

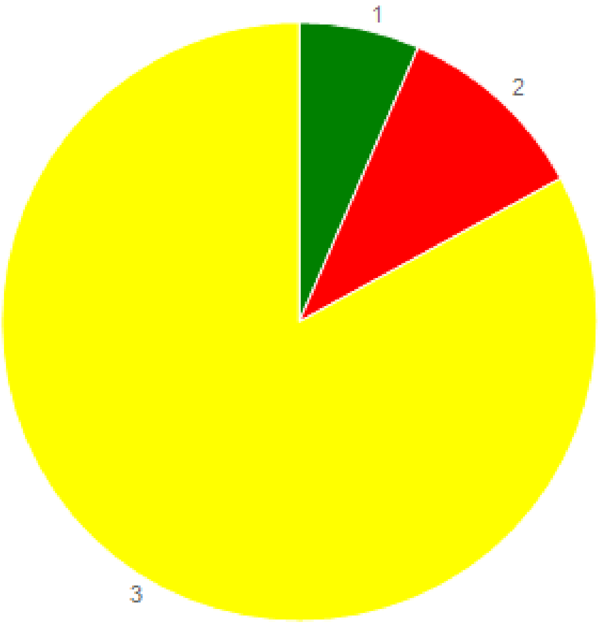
Report Details

Report By: Paul Etnire

Accuracy Count: 3

Time Frame: From 01-01-17 To 01-31-18

Total Hits: 352



Contributor	Score	Hits
1	Correct Hits	23
2	InCorrect Hits	37
3	NotScore Hits	292

Agency
Dashboard Detection Report

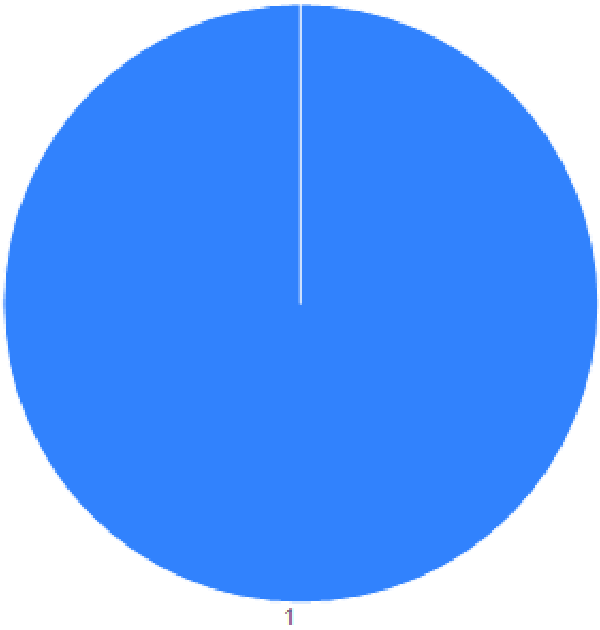
Report Details

Report By: Paul Etnire

Agency Count: 1

Time Frame: From 01-01-17 To 01-31-18

Total Detections: 401,980



Contributor	Agency	Detections
1	My Agency	401,980

Hit Ratio

Dashboard Hit Ratio Report

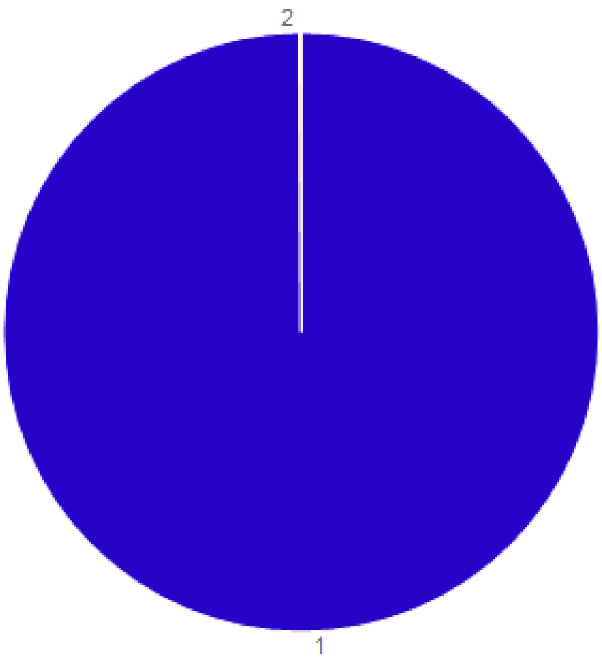
Report Details

Report By: Paul Etnire

Hit Ratio Count: 2

Time Frame: From 01-01-17 To 01-31-18

Total Records: 401,980



Contributor	Record Type	Records
1	Detections	401,628
2	Hits	352

LEARN

Hot-List Records

Dashboard Hot-List Report

VIGILANT SOLUTIONS

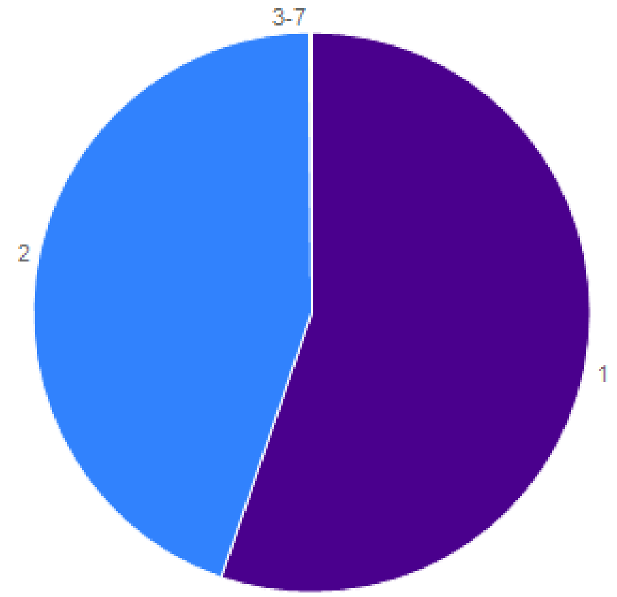
Report Details

Report By: Paul Etnire

Hot-List Count: 7

Time Frame: From 01-01-17 To 01-31-18

Total Hot-List Records: 492,704



Contributor	Source	HotList Records	Date of Load
1	AZ DPS ACIC	272,346	10-23-18
2	DC_ACIC	219,751	05-08-18
3	LEARN	296	09-28-18
4	CDMS Client	271	10-23-18
5	FBI National Hot-List	24	09-17-18
6	LEARN_Arizona Department of Public Safety	15	10-23-18
7	AZDPS	1	04-17-18

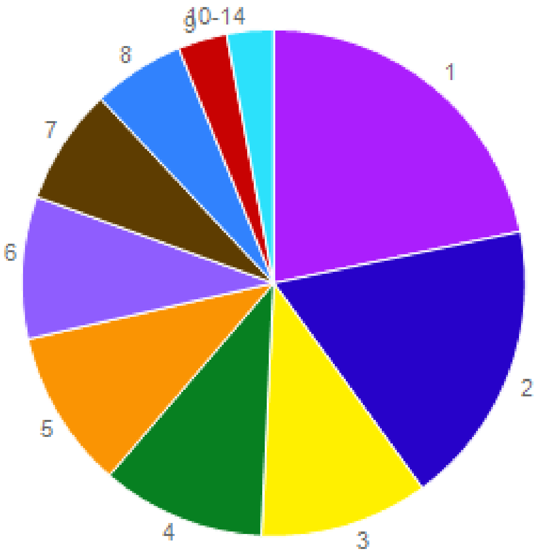
Report Details

Report By: Paul Etnire

System Count: 14

Time Frame: From 01-01-17 To 01-31-18

Total Detections: 401,980



Contributor	System	Detections
1	DPS119095	87,416
2	DPS119094	73,237
3	DPS119930	43,481
4	DPS110248	42,285
5	DPS119101	40,810
6	DPS108830	36,443
7	DPS119090	29,902
8	DPS119091	23,684
9	DPS119096	12,671
10	DPS108828	6,050
11	DPS119007	3,422
12	DPS119009	2,546
13	DPS Mobile Unit	25
14	DPS114190	8

User
Dashboard Detection Report

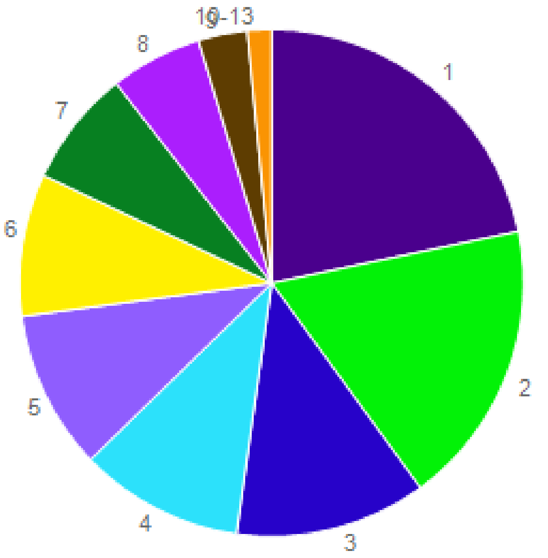
Report Details

Report By: Paul Etnire

User Count: 13

Time Frame: From 01-01-17 To 01-31-18

Total Detections: 401,980



Contributor	User	Detections
1	Brandon Dyson	87,412
2	Robert Huijkman	73,214
3	Kenneth Nix	49,378
4	Wesley Henson	42,285
5	Trooper Shewey	40,795
6	greg andersen	36,443
7	Trooper Yartym	29,902
8	Roderick Whitewater	23,684
9	Elias Johnson	12,671
10	PHIL MOORE	3,444
11	LAN LE	2,544
12	Dion Emory (Deleted)	195
13	Mang Vinh	13

ELSAGNorthAmerica
A Finmeccanica Company

Mobile Plate Hunter-900

ELSAG Operations Center Administrator's Guide

Publication Number MPH-900-OCUM • Version 5.3 • July 2014

Notice
Every effort was made to ensure that the information in this document was accurate at the time of printing or electronic distribution. However, all information is subject to change without notice.

Trademark Information
EOC™ is a trademark of ELSAG North America, LLC.
FPH-900™ is a trademark of ELSAG North America, LLC.
LPRCore™ is a trademark of ELSAG North America, LLC.
MPH-900® is a registered trademark of ELSAG North America, LLC.

ELSAG North America Contact Information
To contact us, please refer to the information below:

Corporate Headquarters — U.S.A.
7 Sutton Place
Brewster, NY 10509
Telephone: 866-9-MPH-900 (866-967-4900)
OR
Telephone: 845-278-5425
Facsimile: 845-278-5428

Technology and Manufacturing
205 H Creek Ridge Road
Greensboro, NC 27406
Telephone: 336-379-7135
Facsimile: 336-379-7164

Technical Support Department
Technical Support Department email: techsupport@elsag.com

Visit us on the Internet
www.elsag.com

Ordering Information
The ordering number for this publication is Publication Number MPH-900-OCUM • Version 5.3. To order this document, contact ELSAG North America.

⚠ **IMPORTANT: If you are in possession of a printed or electronic version of this user's guide, be aware that it may not be the current version. To ensure that you are using the most up-to-date version of this user's guide, please contact ELSAG North America.**

Table of Contents

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

List of Figures

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

List of Tables

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Chapter 1 — General Information

About This Manual

This manual contains information about the ELSAG North America Operations Center System. It covers the various parameters of the application including instructions for daily operation of the system. The intended audiences for this manual include ELSAG North America's customers' general operating personnel, system administrators, authorized ELSAG North America clients and business partners, and Software Product Evaluators. It is primarily focused on the tasks required for day-to-day operation of the system.

Revision Information

If it becomes necessary to revise this installation guide, ELSAG North America will give the reasons for the revision in this section.

Version	Description	Revised Date	Revised By	Approved By
1.0	First release	6/30/2012	DC	CT, NW
1.1	Updated	7/24/2012	DC	CT, NW
1.2	Updated, added cross search, convoy search	9/28/2012	DC	CT, NW
2.0	Updated, TOC, cross search, convoy search	10/24/2012	MM	CT, NW
3.0	Updated for EOC 5.0 Release	8/09/2013	CT	CT, NW
4.0	Updated for EOC 5.2 Release	2/28/2014	LR, CW	LR, SM
5.3	Updated for EOC 5.3 Release	7/31/2014	LR	LR, SM

Table A — Manual Revision Information (English Version)

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

ELSAG North America Terminology, Acronyms, and Terms

The following terms include acronyms that may appear throughout this and other ELSAG North America publications; however, they are terms with which a beginning user may not be familiar.

Term	Explanation/Definition/Description
Alarm	A read whose license plate number matches a List entry.
CarSystem	The vehicle or FCU PC application which allows operator interaction with reads, alarms and lists.
CSV	**C**omma-**S**eparated **V**alue
EOC	**E**lsag **O**peration **C**enter
FCU	**F**ield **C**ontrol **U**nit – Electronic cabinet connected to up to 4 LPR Fixed Cameras and, normally, a computer running the CarSystem application.
GPS	**G**eo **P**ositioning **S**ystem
GUI	**G**raphical **U**ser **I**nterface (pronounced GOO-ee)
IIS	**I**nternet **I**nformation **S**ervices
LAN	**L**ocal **A**rea **N**etwork
List	Any collection of license plate numbers.
LPR	**L**icense **P**late **R**eader or **L**icense **P**late **R**eading
MDT	**M**obile **D**ata **T**erminal
MPH	**M**obile **P**late **H**unter
MWP	ELSAG Middleware
PC	**P**ersonal **C**omputer
Read	The data packet associated with an LPR read event which includes the license plate, GPS location, timestamp, JPEG black and white image of the plate and JPEG color overview of the vehicle.
Reader	Collection of cameras at the same location.
TOC	**T**actical **O**peration **C**enter
USB	**U**niversal **S**erial **B**us

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Chapter 2 — System Overview

Introduction

The ELSAG Operations Center (EOC) manages a fleet of MPH-900 mobile LPR units and/or a network of Fixed LPR cameras. The EOC uploads and archives both read and alarm data coming from all the vehicles and fixed cameras. The EOC software includes a Web site that allows remote access to data. The EOC also manages distribution of the wanted plates database or lists to LPR units.

System Architecture

Figure 1 shows the general system architecture. The EOC Server stores data in a central database. The MPH-900 LPR camera systems mounted on vehicles or connected to an FCU transmit their data wirelessly through a secure Access Point or a wired network connection to the EOC. A secondary Network Interface Card (NIC) of the EOC Server is connected to the existing building LAN, allowing multiple access points to the Operations Center functionality.

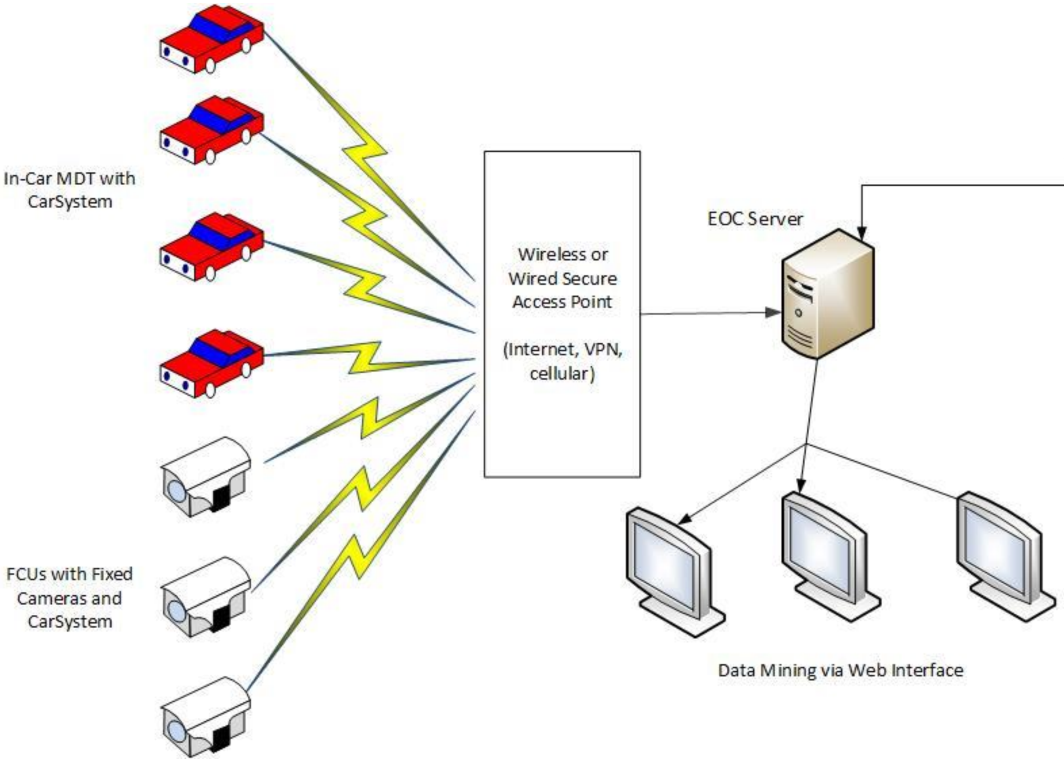
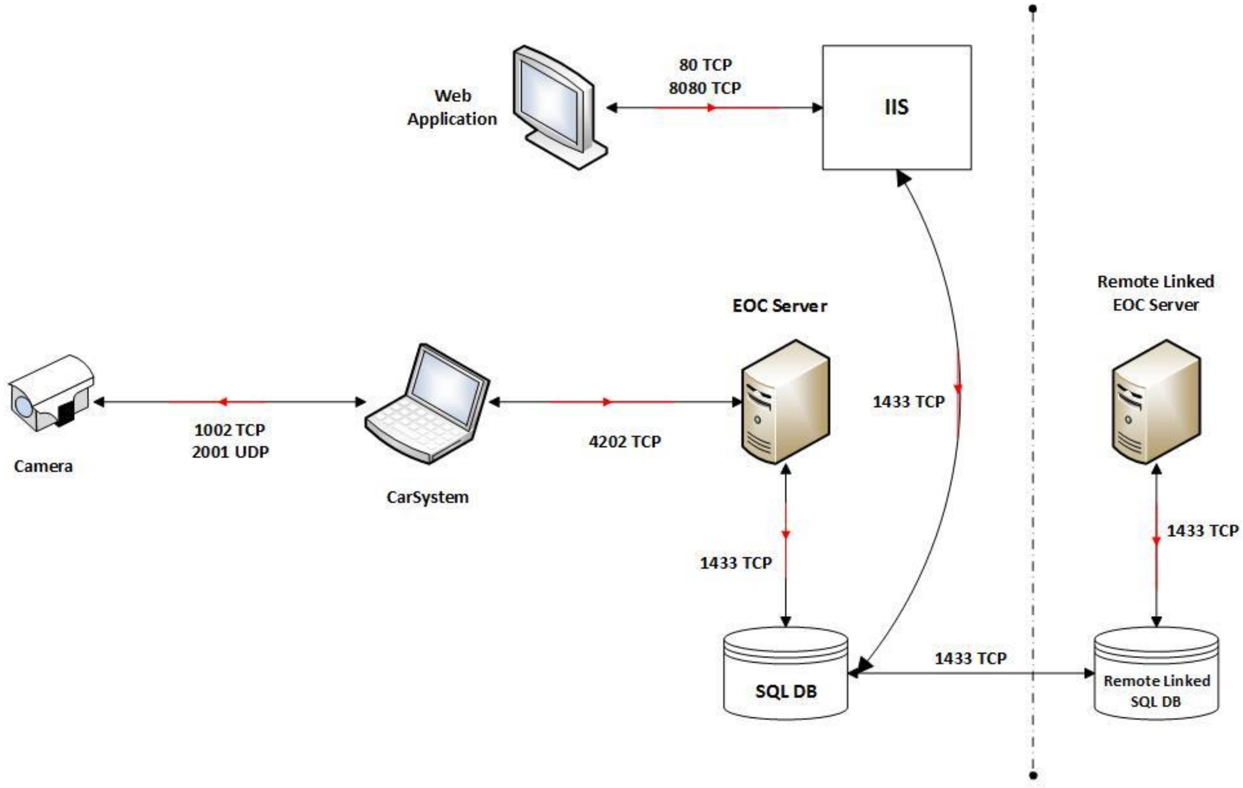

In-Car MDT with CarSystem
FCUs with Fixed Cameras and CarSystem
Wireless or Wired Secure Access Point
(Internet, VPN, cellular)
EOC Server
EOC System Administration
Data Mining via Web Interface

Figure 1 — General System Architecture

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Communication Port Information

EOC and CarSystem components use certain default ports to communicate. Figure 2 illustrates the components, the ports they use by default, and the direction in which communication is initiated.



CarSystem and EOC Components Showing Default Communications Ports

(red arrows show direction in which connection is initiated)

Figure 2 — Components, Ports, and Communications Direction

NOTE: The use of port 4200 between CarSystem and EOC server for diagnostics was discontinued after EOC 4.2.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

The same information is summarized below in Table B.

Table B — Components, Ports, and Communications Direction

Component and Path	Default Port(s)	Connection Direction
Camera to CarSystem	1002 TCP for data 2001 UDP for diagnostics	From CarSystem to Camera
CarSystem to/from EOC Server	4202 TCP for data	From CarSystem to EOC Server
EOC Server to/from SQL DB	1433 TCP	From EOC Server to SQL DB
EOC Web application to/from IIS	80 TCP for data 8080 TCP for maps	From Web application to IIS
IIS to/from SQL DB	1433 TCP	From IIS to SQL DB
SQL DB to/from Remote Linked SQL DB	1433 TCP	Either direction

Configuring Cameras

For information about how to configure the cameras' firmware, see the *Mobile Plate Hunter-900 CarSystem Installation Guide*, Publication Number MPH-900-CSIG.

The CarSystem installation process will normally configure and connect the cameras to the EOC automatically. To configure the cameras' connections to the EOC manually or to add a new camera, see the *Mobile Plate Hunter-900 CarSystem User's Guide*, Publication Number MPH-900-CSUG.

EOC Modes

The EOC system operates in two authentication modes: **SQL Server Mode** and **Active Directory Mode**.

SQL Server Mode requires you to create users in the EOC's SQL Server database and use those accounts to manage login authentication. In essence, the EOC handles user authentication independently of the Microsoft[1] Windows[2] domain network.

Active Directory Mode uses the Microsoft Active Directory, a service for Windows domain networks that serves as a central mechanism for network administration and security. In Active Directory mode, the EOC authenticates users using Active Directory, i.e., Windows domain user accounts. That is, the Windows system enforces authentication independently of the EOC.

Note that, although user authentication and management are performed through Windows, you will need to set up accounts within the EOC to map to those Windows user accounts. See *Logging in to the EOC — Active Directory Mode* for details.

The mode in which your implementation of EOC operates is set up at installation time. You will not be able to alternate between the two modes in an installed EOC system.

[1] Microsoft® is a registered trademark of Microsoft Corporation.

[2] Windows® is a registered trademark of Microsoft Corporation.

Active Directory Mode — Differences

There are two significant ways in which Active Directory Mode differs from SQL Server Mode. Both are related to the fact that, in Active Directory Mode, user authentication and user management are performed by the Windows system, not by the EOC.

- User login in Active Directory Mode is detailed in *Logging in to the EOC — Active Directory Mode*.
- Creating and managing users in Active Directory Mode is detailed in *Managing Users — Active Directory Mode*.

Accessing EOC Functionality

Once a user logs in, the main menu of the EOC will only display those EOC functions that the user has permissions to perform.

If you have full permissions to the system, you will see the following top-level menu shown in Figure 3 when you log in.

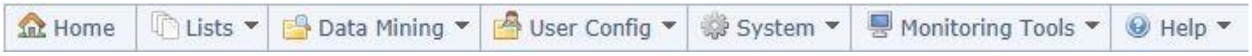


Figure 3 — EOC Main Menu

Below is a description of each selection on the EOC Menu and their uses.

> **NOTE**: If your system has been configured to limit your access to certain system functions, you may not see all of the following menu selections.

Lists

The Lists Drop Down Menu is shown below in Figure 4.

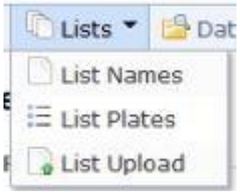


Figure 4 — Lists Drop Down Menu

- **List Names**
  - Creates, edits, deletes and views the structure and characteristics of lists (not the data itself).
- **List Plates**
  - Searches for a plate in a list by plate number, state and/or alarm class
  - Views the details of the plate entry in the list
  - Changes some information about the entry

- Creates a list entry, and
- Deletes a plate entry.

❑ **List Upload**

- Sets the parser file to be used to format incoming list data
- Shows sample format for parser file, and
- Uploads a list to refresh the data.

Data Mining

The Data Mining Drop Down Menu is shown below in Figure 5.

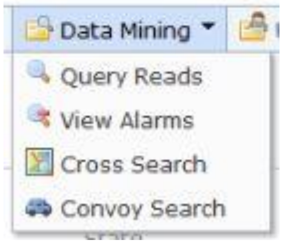


Figure 5 — Data Mining Drop Down Menu

❑ **Query Reads**

- Views plate read information and details, including images.
- Creates data sets of plate reads using filters for date, time, plate number, state, location, source, status, alarm class and/or domain.
- Uses maps to display the geographic location of plate reads, and
- Exports data sets to comma-separated value (CSV), PDF format or HTML files.

❑ **View Alarms**

- Views alarm information and details, including images
- Creates data sets of alarms using filters for date, time, plate number, make, model, state, location, source, status, alarm class and/or domain.
- Uses maps to display the geographic location of alarms, and
- Exports data sets to comma-separated value (CSV), PDF format, or HTML files.

❑ **Cross Search**

- Cross search allows you to compare the results of multiple queries (up to five) to determine if plate reads are duplicated within a time range or across different time ranges, in the same location or in different locations.
- Determine if one or more vehicles was present at a specific location during a different time frame, and

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

  - Determine if the same vehicle or vehicles was present at different locations during different time frames.

- **Convoy Search**
  - The Convoy Search feature allows you to identify plates that are seen together frequently.

User Config

The User Config Drop Down Menu is shown below in Figure 6.

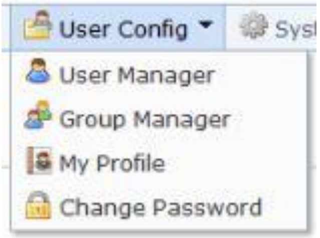


Figure 6 — User Config Drop Down Menu

- **User Manager**
  - Creates, edits, deletes and views the characteristics of EOC users, filtering by user name, domain, email address, creation time and date, and whether the user is locked or enabled (includes changing user passwords).
- **Group Manager**
  - Creates, edits, deletes and views the characteristics of EOC groups for Feature and Domain privileges, filtering by group name, domain, description and session timeout.
- **My Profile**
  - Sets up email notifications of alarms for accessible lists, failed system tasks and additional Email distribution lists.
- **Change Password (SQL Server Mode only)**
  - Changes your own password.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

System

The System Drop Down Menu is shown below in Figure 7.

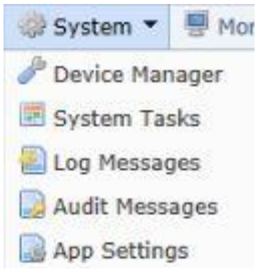


Figure 7 —System Drop Down Menu

- ❑ **Device Manager**
  - ■ Creates, views, edits, and deletes system configuration (domains, cars, cameras, FCUs, etc.).
- ❑ **System Tasks**
  - ■ Schedules, runs and manages system maintenance tasks, and
  - ■ Reports on system task status.
- ❑ **Log Messages**
  - ■ Collects a list of all system messages from all devices.
- ❑ **Audit Messages**
  - ■ Collects a list of all searches and changes made and who performed them.
- ❑ **App Settings**
  - ■ General EOC application settings for Language, default map latitude and longitude, Default Convoy Search interval, TOC Active Alarm Duration, Require Reason for Query and Alarm Validation.
  - ■ SMTP settings for sending Email alerts.
  - ■ SQL Membership Provider sets password constraints.
  - ■ Data Retention sets policies for Audit and Log Messages, Reads and Alarms data retention.
  - ■ Safe Mode access and user Membership Provider information.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Monitoring Tools

The Monitoring Tools Drop Down Menu is shown below in Figure 8.

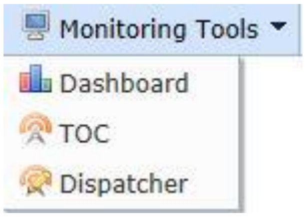


Figure 8 — Monitoring Tools Drop Down Menu

- ❑ **Dashboard**
  - ■ Dashboard is a utility for system administrators and technicians that need to observe current performance details of the EOC system, and
  - ■ Totals, Reads, Alarms, Failed, List Status, GPS Status, Time Difference, Statistics Report, and Statistics Builder.
- ❑ **TOC (Tactical Operations Center)**
  - ■ The Tactical Operations Center (TOC) EOC plug-in feature displays recent alarms. Alarms generated from cars or fixed cameras feed back to the EOC server, which populate the most recent alarms list on the TOC screen.
- ❑ **Dispatcher**
  - ■ The EOC Dispatcher allows users to view real-time alarms from mobile and fixed camera sites with the ability to Correct/Incorrect each alarm record, Edit and add Officer Notes.

Help

- ❑ **About**
  - ■ Describes the EOC product.

Chapter 3 — Authentication and Login

Introduction — Authentication and Login

Once the ELSAG North America Operations Center is installed, you'll need the following information to log in for the first time:

- URL of the EOC System, and
- The default username and password.

The default user will have maximum permissions (set by the default group) within the EOC database; in essence, the default user is a system administrator-level user, able to create domains, groups, and users.

The EOC system operates in two authentication modes: **SQL Server Mode** and **Active Directory Mode**. The primary difference is that in **SQL Server Mode**, authentication is performed by the SQL Server database. In **Active Directory Mode**, authentication is performed by Windows Active Directory.

The two modes have similar functionality, but the user interface is organized in slightly different ways.

Default Installed Account, Password, and Permissions

The EOC is installed with a default domain, user and group. The group sets the maximum permissions for the default user, so this user is, in effect, the system administrator account for the system.

The installation process creates a default domain, a default group, and at least one default user in that group. The default domain is named **Administrative**; the default group is named **Administrators**. The default user is named **Administrator** and the default password for that account is **defaulteocpassword**.

Password Parameters and Requirements

If you are operating in SQL Server Mode, your user accounts will have the following restrictions:

- Passwords must be a minimum of six characters in length, using any alphanumeric and/or special characters, and
- Five (5) incorrect login attempts will lock a user out of the system, in which case the system administrator will have to re-enable the account.

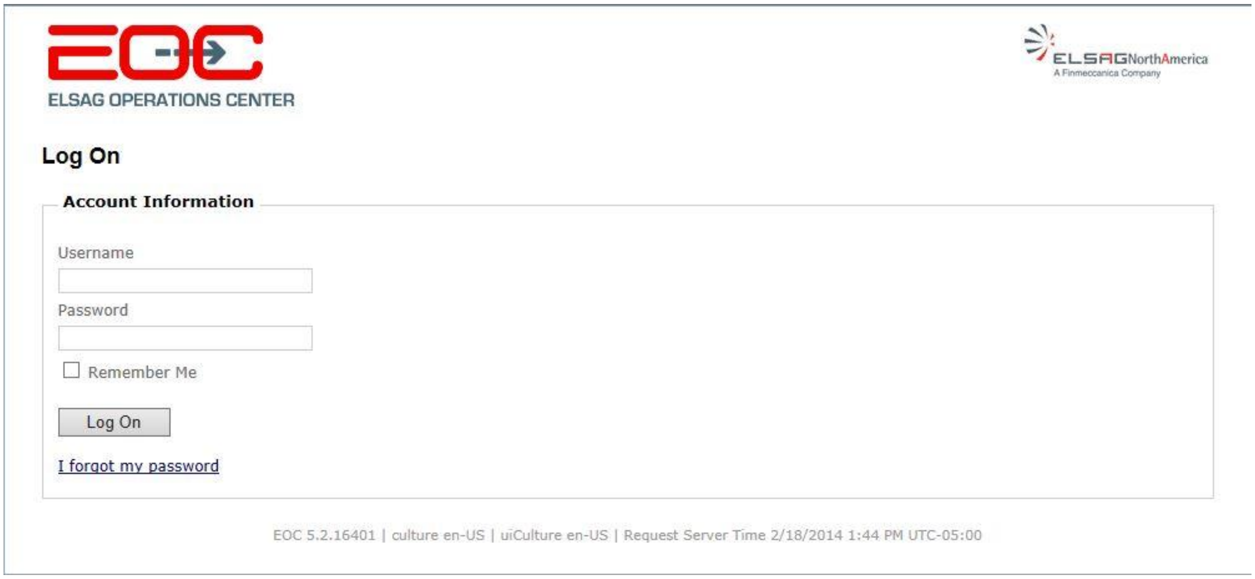
  NOTE: The time window in which consecutive failed attempts are tracked is ten (10) minutes. Thus, if you try four times and fail, then wait ten minutes, the system will see your next attempt as the first, not the fifth. Password constraints can be modified using the **SQL Membership Provider** option described on page 136.

If you are operating in Active Directory Mode, the only restrictions on passwords are those enforced by your Windows Active Directory system. There is nothing in the EOC that you can do to change them.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Logging in to the EOC — SQL Server Mode

To log into the EOC system, navigate to the URL of the Web site where the EOC resides. Be sure to make a note of the EOC URL and add it to your Web browser's **Favorites**. Referring to Figure 9, the screen you will see will be the Login Screen. To login follow the steps below.



Log On

Account Information

Username

Password

□ Remember Me

Log On

I forgot my password

EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:44 PM UTC-05:00

Figure 9 — Login Screen (SQL Server Mode)

(1) Enter your Username and Password in the correct fields.

NOTE: If you are not a system administrator, your administrator will email you a login name and a temporary password when he or she sets up your user account. If you are a system administrator, you can log in for the first time using the default installed administrator account.

(2) Select the **Remember me** checkbox so that you will not need to reenter your username every time you log in.

(3) If you have forgotten your password, press the **I forgot my password** link. The system will email a new password you can use to reset your password, to the email address associated with the EOC user account.

(4) Press the **Log On** button.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Logging in to the EOC — Active Directory Mode

Because authentication in Active Directory Mode is handled by Windows Active Directory, logging into the EOC in Active Directory Mode is slightly different from logging in to an EOC in SQL Server Mode. To log into the EOC system, navigate to the URL of the Web site where the EOC resides. Be sure to make a note of the EOC URL and add it to your Web browser’s **Favorites**. Referring to Figure 10, the screen you will see will be the Login Screen. To login follow the steps below.

> **NOTE:** You log into Active Directory Mode using your standard Windows username (in the form of *DOMAIN\username* or *username*) and the password.

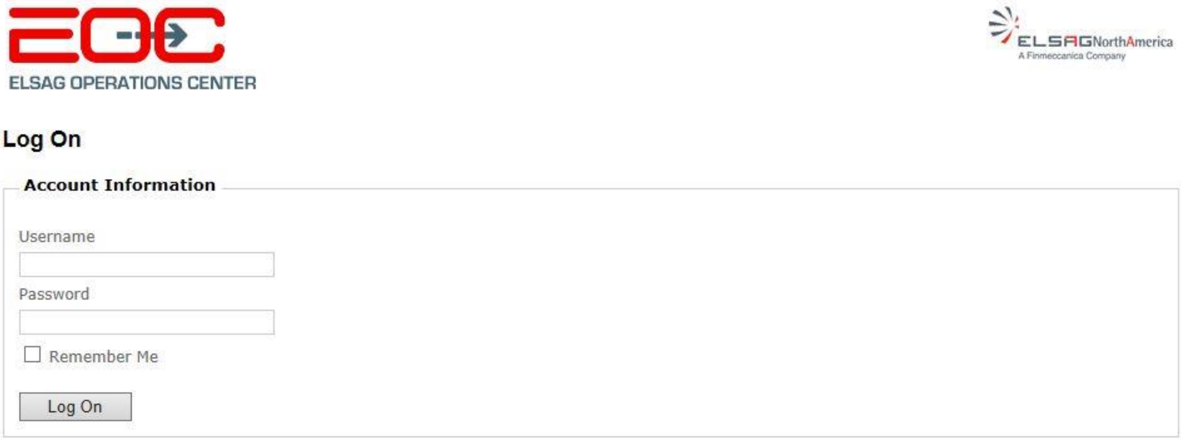


Figure 10 — Login Screen (Active Directory Mode)

(1) Enter your Windows username and password in the correct fields.

(2) Select the **Remember me** checkbox so that you will not need to reenter your username every time you log in.

(3) Press the **Log On** button.

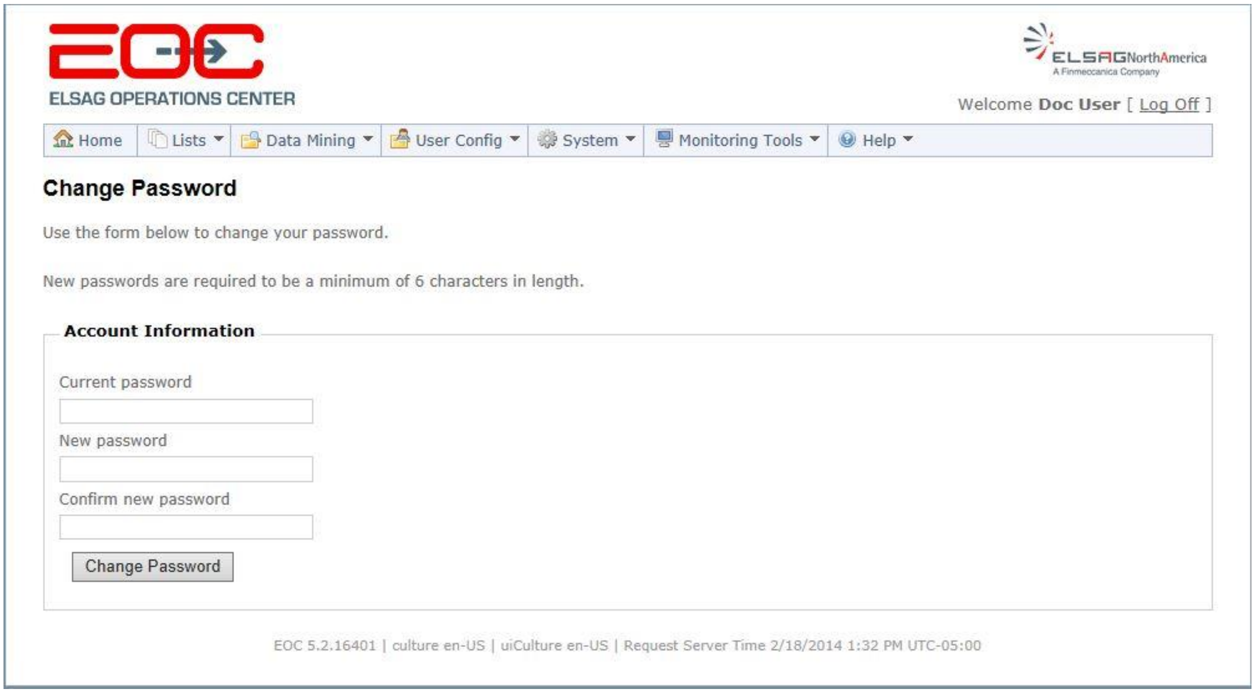
NOTE: There is no **I forgot my password** link, since authentication and user management is handled through Windows and not through the EOC.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

First Time User Changes Password Procedure

The first time you log in while in SQL Server Mode, you will be prompted to change your password, as shown below in Figure 11. Continue to the next section for the procedure to change your own password.

> **NOTE:** If you do not change your password, you will still be allowed access to the system, but you will be prompted to change the password every time you subsequently log in. It's better practice to change the password the first time you log in.



Change Password

Use the form below to change your password.

New passwords are required to be a minimum of 6 characters in length.

Account Information

Current password

New password

Confirm new password

EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:32 PM UTC-05:00

Figure 11 — Change Password Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Change Your Own Password Procedure

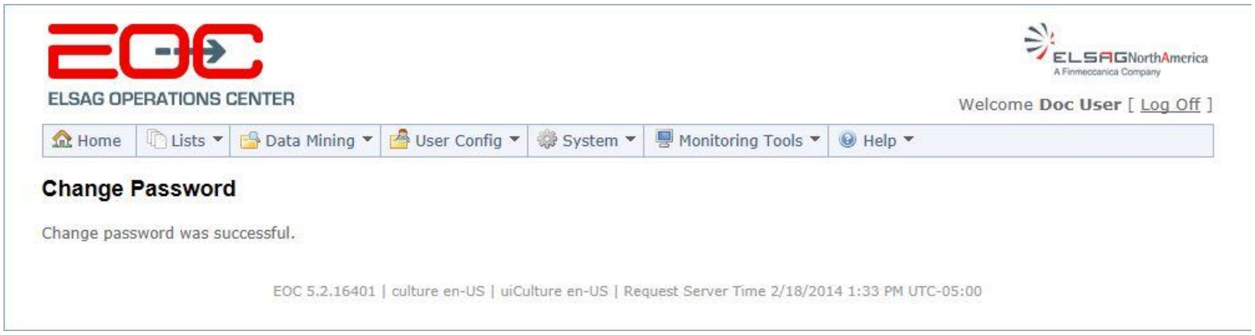
To change your password the first time you log in, perform the steps that follow:

(1) Enter the default password your system administrator sent you in the **Current password** text box.

(2) Type the new password into the **New password** text box.

(3) Type the new password into the **Confirm new password** text box.

(4) Press the **Change Password** button and the screen shown in Figure 12 will appear.



Change Password

Change password was successful.

EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:33 PM UTC-05:00

Figure 12 — Change Password Success Message

Safe Mode

Safe mode is a default system account that always allows you to log in, even if you've somehow broken your permissions in such a way that a regular administrative account will not login.

You must log into Safe Mode on the physical machine where the EOC resides (i.e., localhost).

Safe Mode is available regardless of whether you are operating in Active Directory Mode or SQL Server Mode.

When you log into Safe Mode, you will lock other users out of the EOC system for the duration of your session. Other users will see a splash screen with the message that the system is undergoing maintenance.

The login name for Safe Mode is: **SafeModeUser**; the default password is **SafeModeUser**. For obvious reasons, this user name and password cannot be changed.

Troubleshooting Using Safe Mode

The EOC provides you a mechanism by which you can recover from serious errors. Safe Mode is a special mode of the EOC that only works on the physical machine in which the EOC is installed. Safe Mode can be accessed two ways.

❑ **Accessing Safe Mode from within EOC**

(1) To log into the system in Safe Mode, go to the physical machine where the EOC server resides and navigate to the correct URL for the EOC server.

(2) Navigate to **System > App Settings > Safe Mode**.

(3) Referring to Figure 13, Click "**Enter Safe Mode**" button.

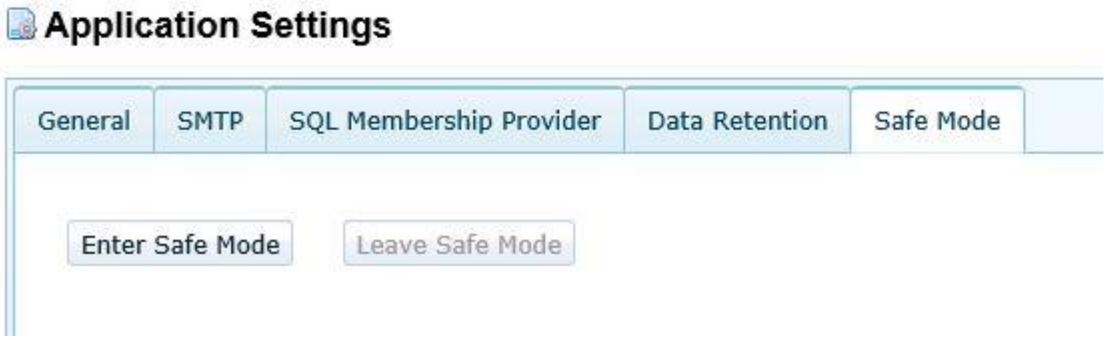
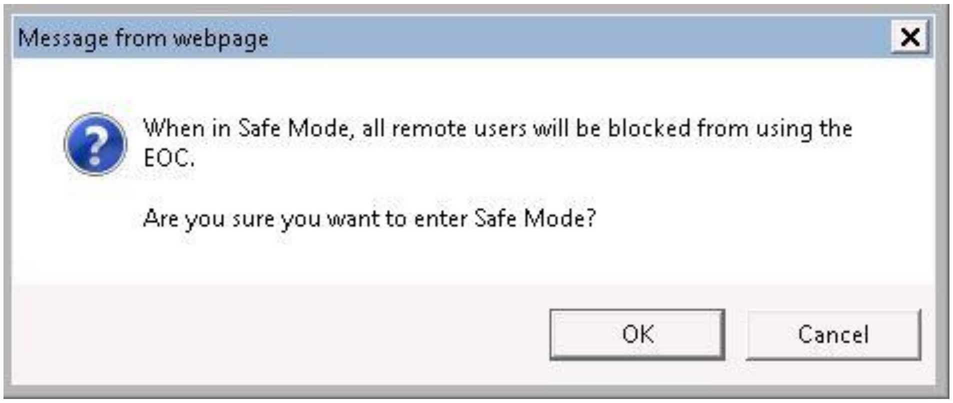


Figure 13 — System App Settings Safe Mode Selection

(4) Referring to Figure 14, click the **OK** button to confirm entering Safe Mode. Click the **Cancel** button to cancel entering Safe Mode


Message from webpage

When in Safe Mode, all remote users will be blocked from using the EOC.

Are you sure you want to enter Safe Mode?

Figure 14 — Entering Safe Mode Warning Message

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(5) Referring to Figure 15, you will automatically be logged in as SafeModeUser.

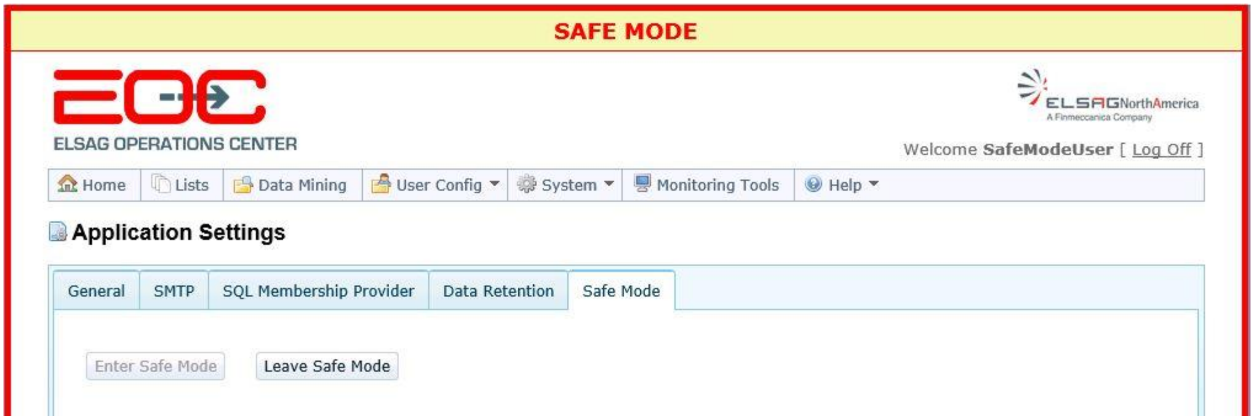


Figure 15 — EOC Safe Mode Enabled

(6) Now you can perform whatever maintenance or error correction you need to do.

(7) Referring to Figure 15, to log out of Safe Mode, navigate to **System > App Settings > Safe Mode**.

(8) Click the "**Leave Safe Mode**" button.

(9) Referring to Figure 16, click "OK" to confirm exiting Safe Mode. The EOC will exit Safe Mode and leave you at the log in screen.

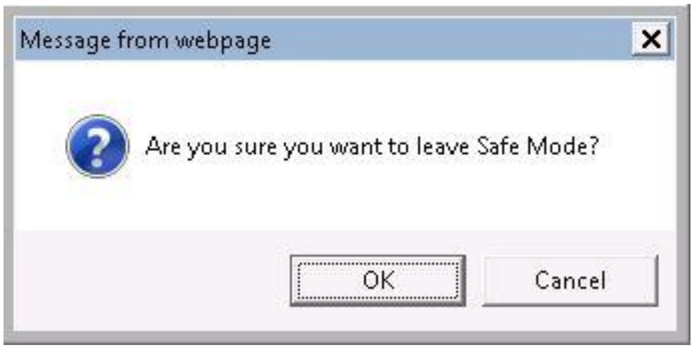

Are you sure you want to leave Safe Mode?

Figure 16 — EOC Exit Safe Mode Confirmation Question

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

❑ Accessing Safe Mode Using IIS

(1) Referring to Figure 17, to log into the system in Safe Mode, go to the physical machine where the EOC server resides and navigate to the correct URL for the EOC server.

(2) Open the IIS Manager by going to **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.

(3) Select the **EOC4 Web** site.

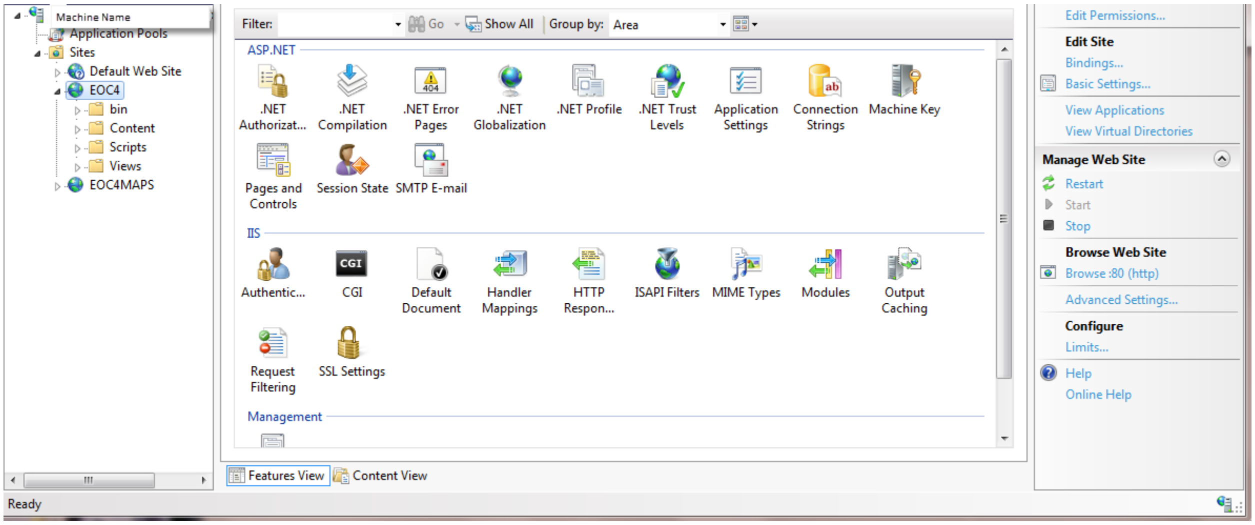


Figure 17 — IIS Manager (Select EOC Site)

(4) Referring to the highlighted icon in Figure 18, double click on **Application Settings** for the Web site.

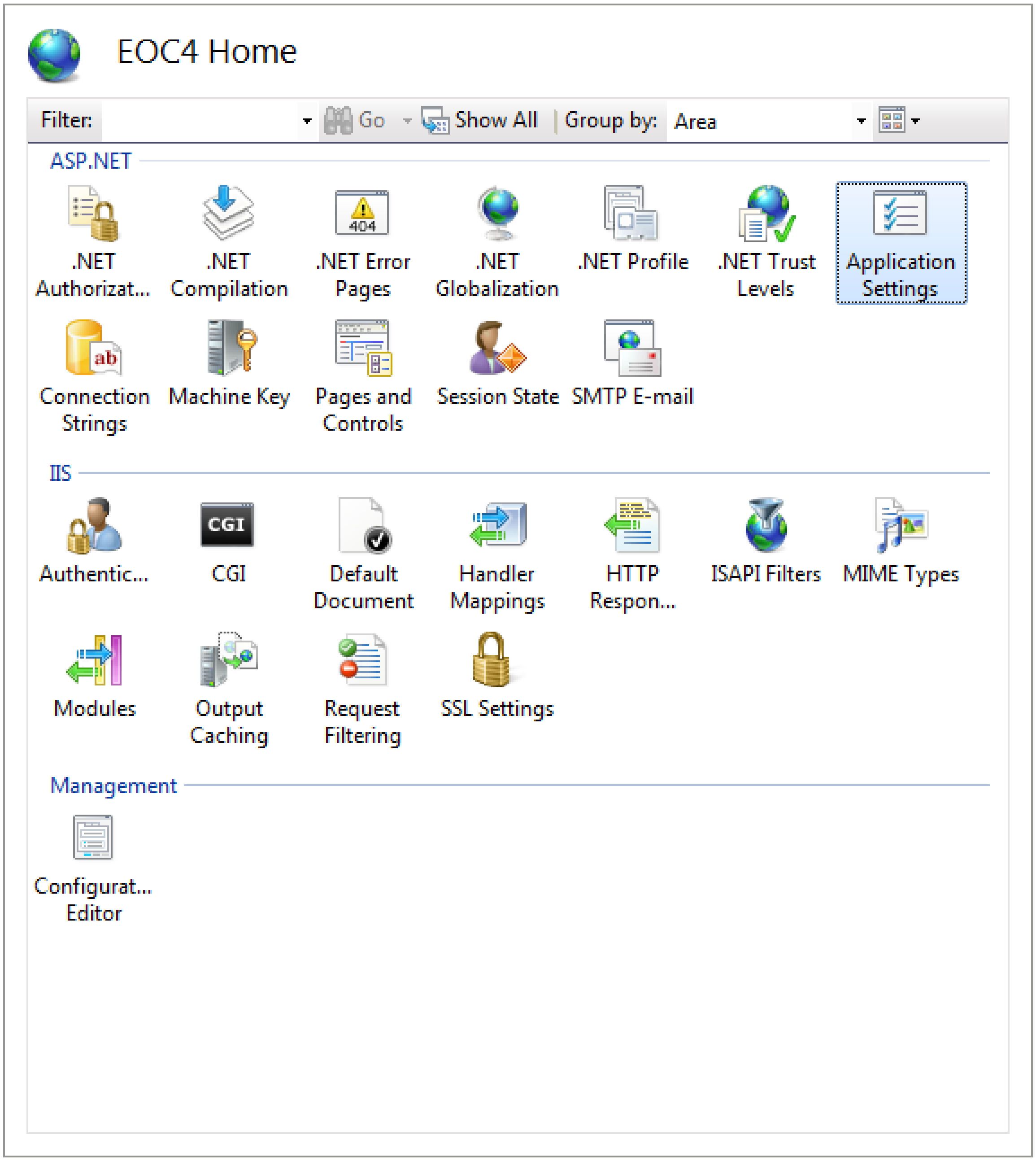
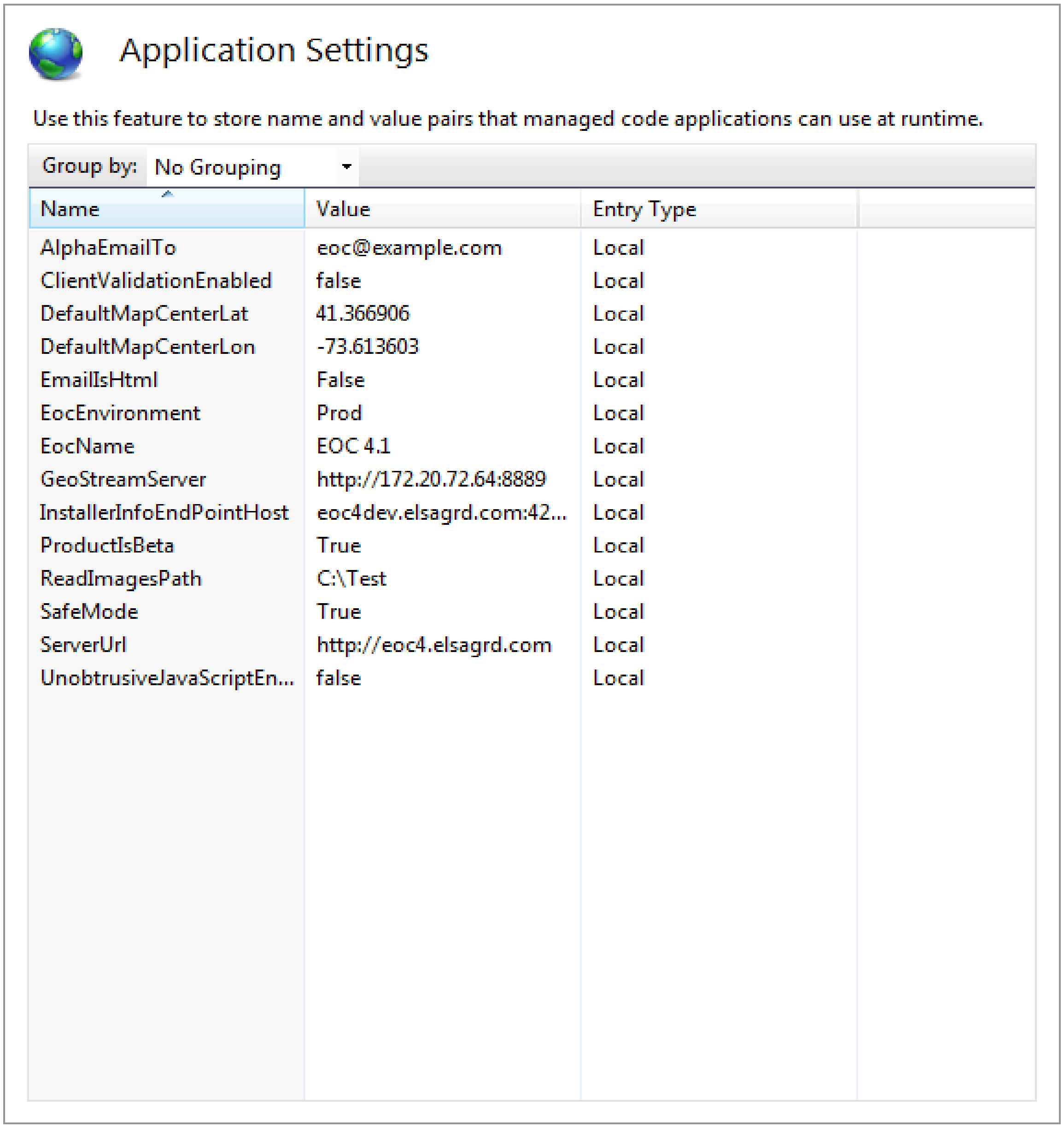


Figure 18 — Application Settings Selected

(5) Referring to Figure 19, you will see a list of settings for the site.



Application Settings

Use this feature to store name and value pairs that managed code applications can use at runtime.

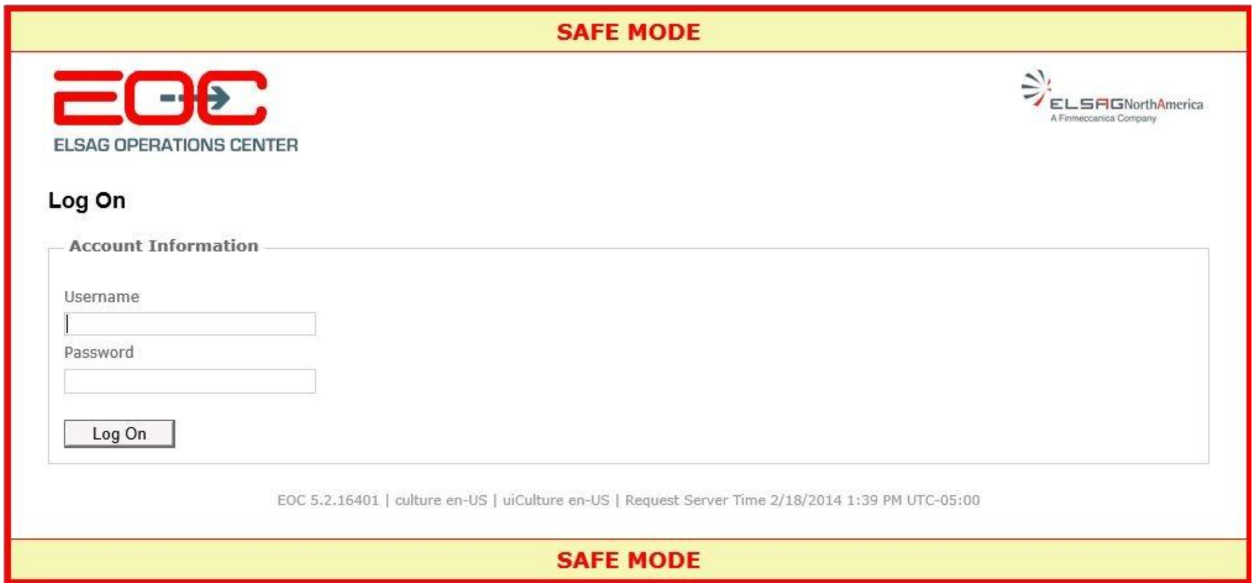
Name	Value	Entry Type
AlphaEmailTo	eoc@example.com	Local
ClientValidationEnabled	false	Local
DefaultMapCenterLat	41.366906	Local
DefaultMapCenterLon	-73.613603	Local
EmailIsHtml	False	Local
EocEnvironment	Prod	Local
EocName	EOC 4.1	Local
GeoStreamServer	http://172.20.72.64:8889	Local
InstallerInfoEndPointHost	eoc4dev.elsagrd.com:42...	Local
ProductIsBeta	True	Local
ReadImagesPath	C:\Test	Local
SafeMode	True	Local
ServerUrl	http://eoc4.elsagrd.com	Local
UnobtrusiveJavaScriptEn...	false	Local

Figure 19 — Application Settings List

(6) Right-click on **Safe Mode** and select **Edit**. Make sure the value reads **True.**

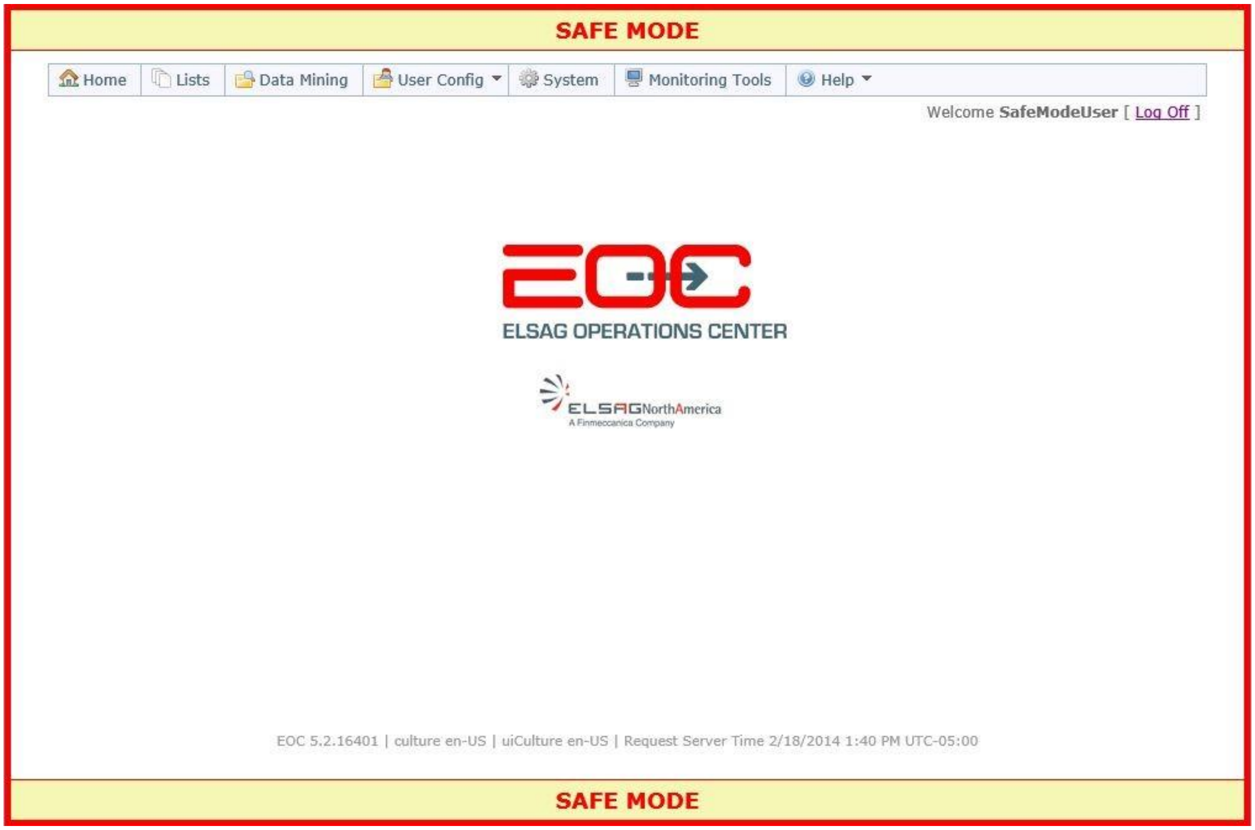
(7) Refresh the EOC URL and the EOC system will show you the **Safe Mode** login screen as shown in Figure 20.

(8) Log into the EOC using the username **SafeModeUser** and the password **SafeModeUser** and the screen shown in Figure 21 will appear.



EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:39 PM UTC-05:00

Figure 20 — EOC Safe Mode Login



EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:40 PM UTC-05:00

Figure 21 — EOC Safe Mode Home Page

(9) Now you can perform whatever maintenance or error correction you need to do.

(10)To log out of Safe Mode, open the IIS Manager by going to **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.**

(11)Select the **EOC4 Web** site (see Figure 22).

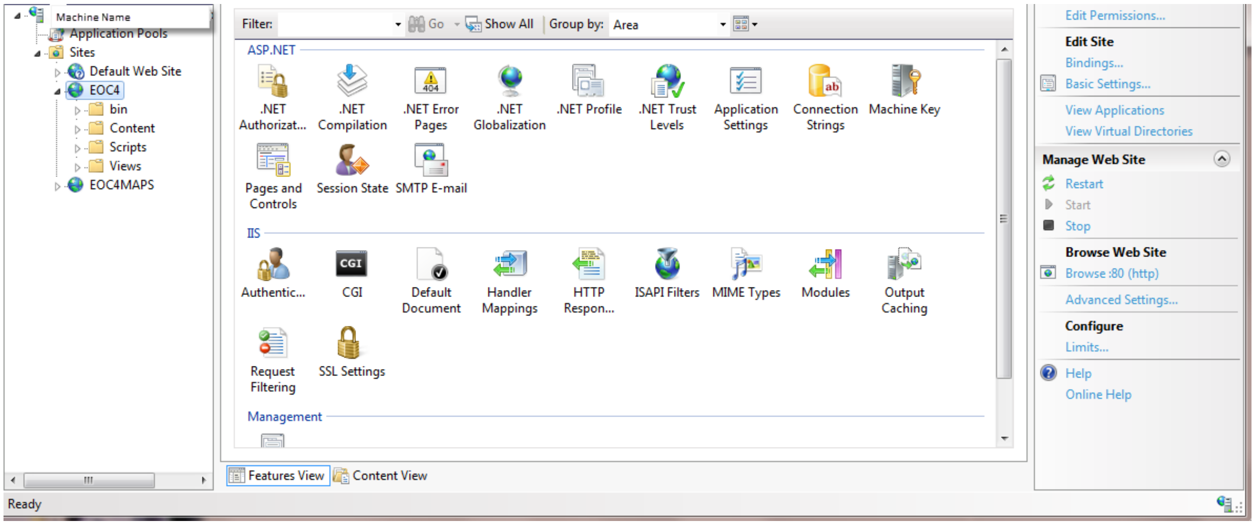


Figure 22 — IIS Manager (Select EOC Site)

(12)Referring to Figure 23, double click on **Application Settings** for the Web site and the screen shown in Figure 24 will appear with this list of settings for the site.

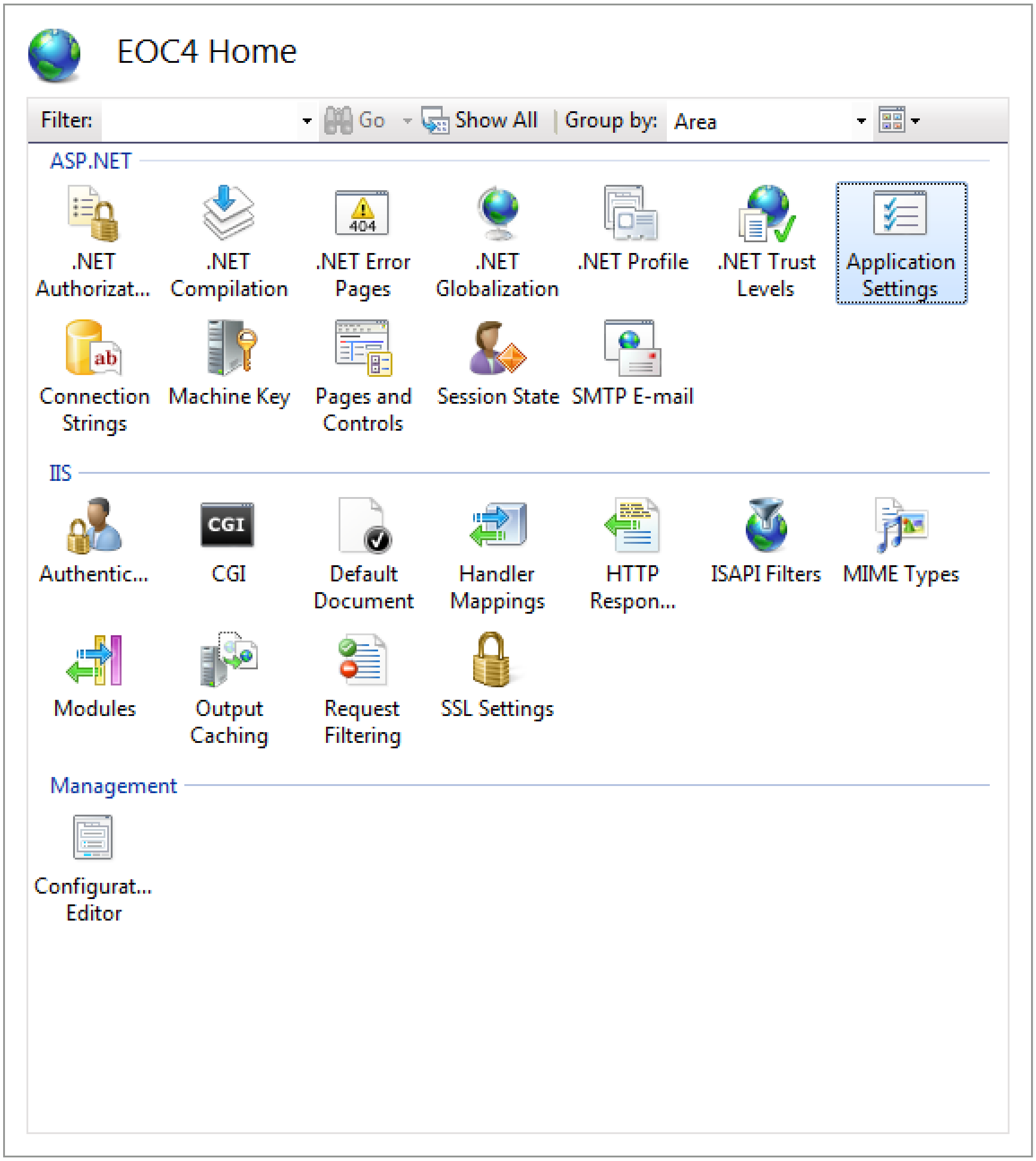
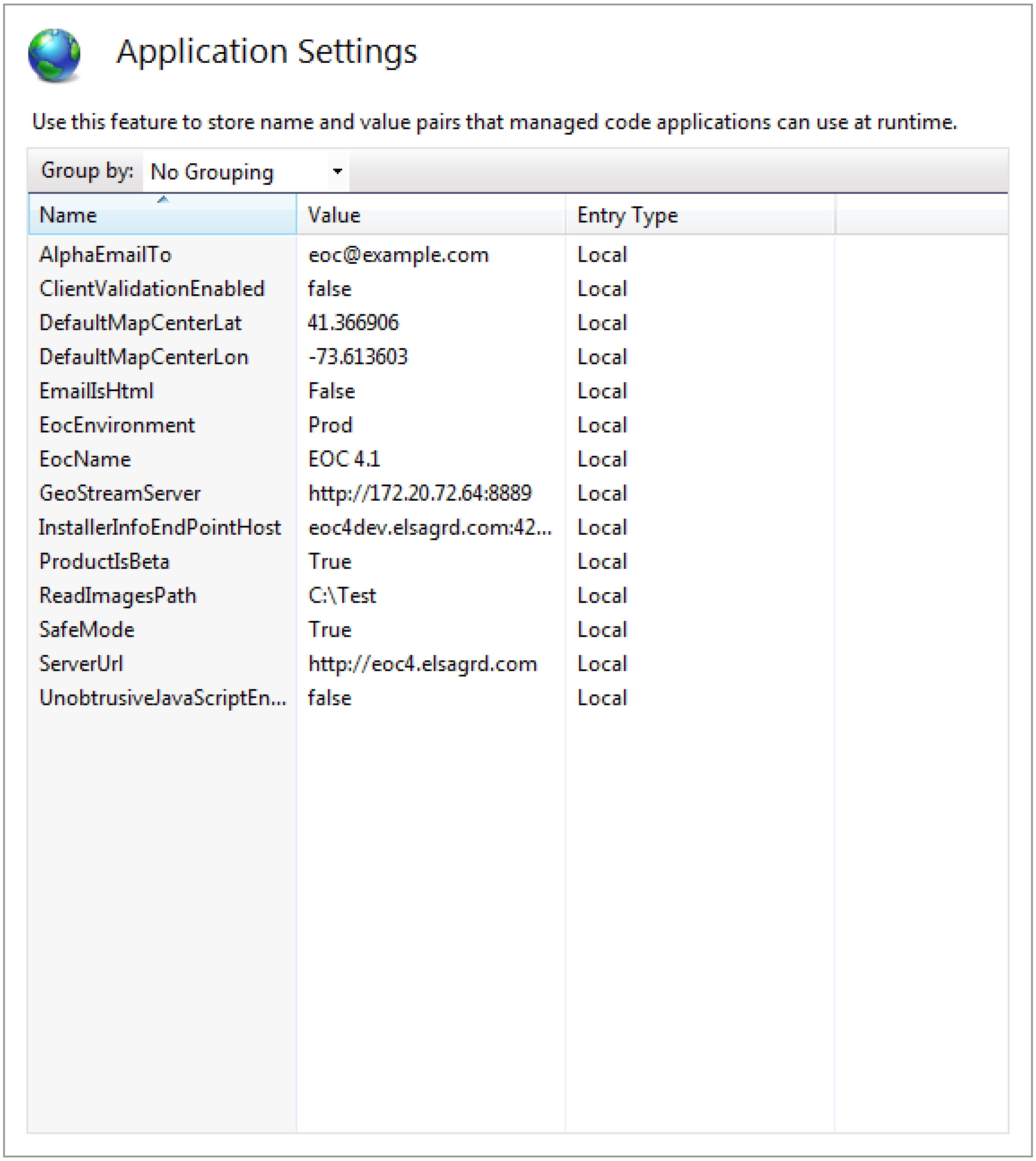

Group by: Area

Figure 23 — Application Settings Selected

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(13)Referring to Figure 24, right click on **Safe Mode** and select **Edit** then change **the Value** to **False.**



Application Settings

Use this feature to store name and value pairs that managed code applications can use at runtime.

Group by: No Grouping

Name	Value	Entry Type
AlphaEmailTo	eoc@example.com	Local
ClientValidationEnabled	false	Local
DefaultMapCenterLat	41.366906	Local
DefaultMapCenterLon	-73.613603	Local
EmailIsHtml	False	Local
EocEnvironment	Prod	Local
EocName	EOC 4.1	Local
GeoStreamServer	http://172.20.72.64:8889	Local
InstallerInfoEndPointHost	eoc4dev.elsagrd.com:42...	Local
ProductIsBeta	True	Local
ReadImagesPath	C:\Test	Local
SafeMode	True	Local
ServerUrl	http://eoc4.elsagrd.com	Local
UnobtrusiveJavaScriptEn...	false	Local

Figure 24 — Application Settings List

(14)Refresh and the EOC system will log out of Safe Mode and prompt you to log in as a normal user.

Getting Started — Domains, Groups, and Users

Once you’ve installed the EOC successfully, you must configure the system in the way in which you plan to use it, by creating and editing domains, users, and groups.

The installation process creates a default domain, a default group, and at least one default user in that group. The default domain is named **Administrative**; the default group is named **Administrators**. The default user is named **Administrator**.

These defaults give you the necessary tools to begin configuring your system.

To configure the EOC, you must follow the following sequence:

- Create the domain first
- Then create a group or groups with permissions on the new domain, and
- Create users and associate them with the group (or groups) to give them appropriate permissions within the EOC.

Domains provide you with a way to categorize data within the EOC server. When you create users and groups, you assign them to a domain. You can also use domains to segregate different kinds of data, such as confidential lists.

Groups control the permissions assigned to users associated with that group. Access to data and EOC functionality depends on the permissions you assign. For example, if you want some users to be able to perform system configuration tasks, you would create one group with permission to do those tasks within the appropriate domain and another without those permissions. Note that groups can span multiple domains.

Chapter 4 — Data Mining

Introduction

Key to the utility of the EOC system is the ability to search the plate data collected by cameras as well as alarms and list data added to the system from various sources.

Beyond the basic search capabilities, EOC also allows you to:

- Save search parameter sets for reuse
- Send a single URL for a completed search to another EOC user, and
- Show both local time and the UTC offset for a particular plate read.

Searching for Plates

Plate Reads and Permissions

As with all data in the EOC system, your access to reads and alarms depends on the permissions you have. For alarms, you must have permissions to the list from which an alarm is generated.

If you search for a particular plate read that has alarms associated with it and you don't have permissions to the list from which the alarm was raised, the search results displayed will only show the result as a read, not an alarm (since that would reveal that the plate was in a list somewhere).

Fast Querying

To perform a Fast Query, use the steps that follow.

(1) Referring to Figure 25, after you have logged in for the first time and changed your password, you will see this screen, which allows you to perform fast querying without going through the **Data Mining** menu. This can be useful in the case where you are only interested in searching for a plate or two in the EOC database and you do not have other EOC work to do.

NOTE: You can also reach this page at any time by selecting **Home**.

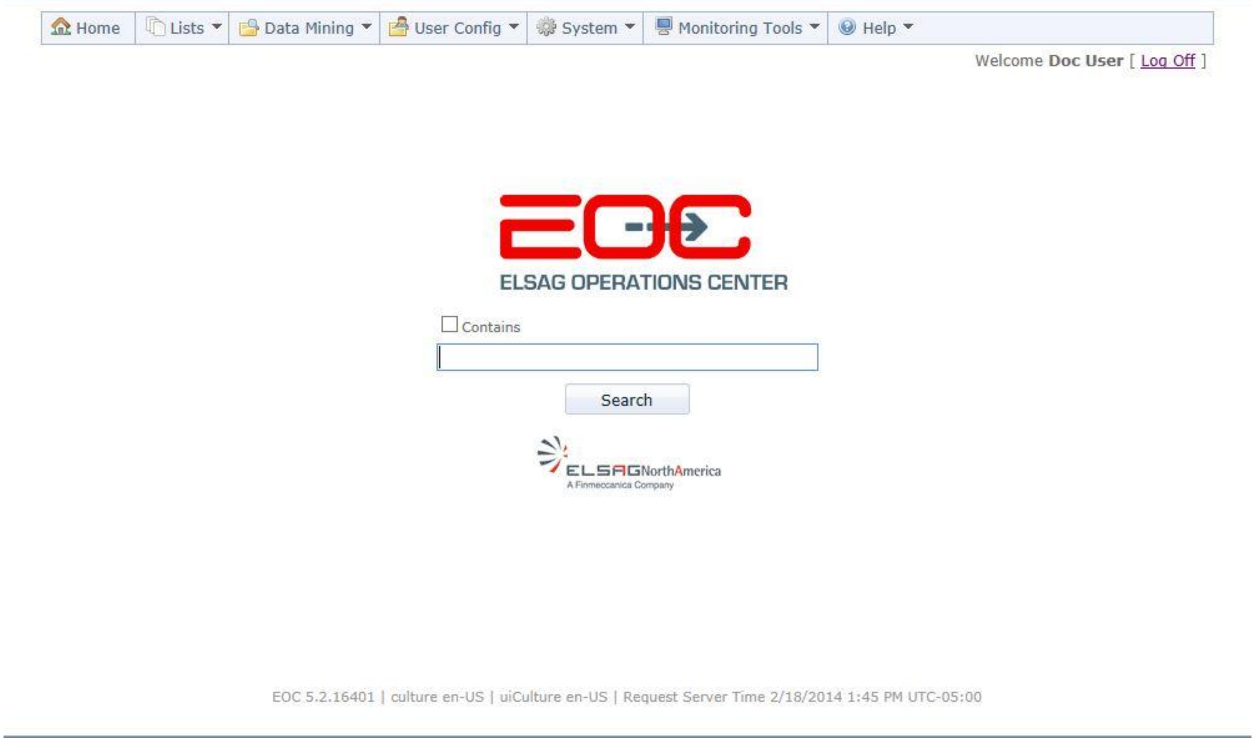
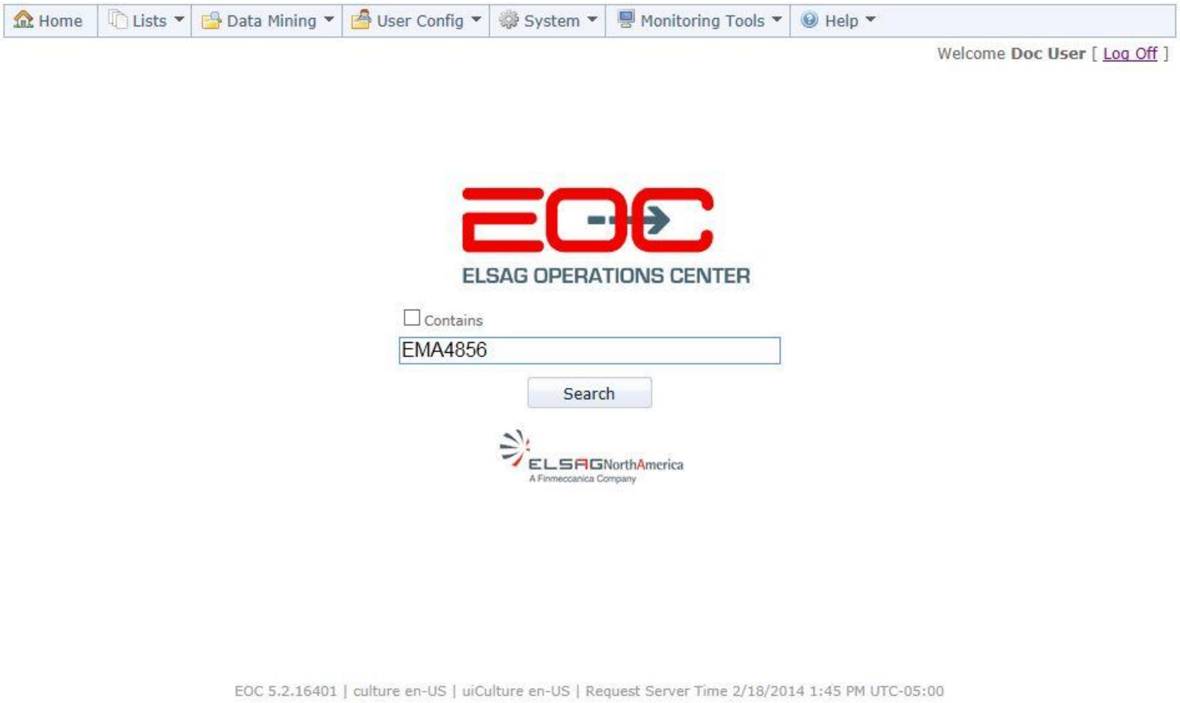


Figure 25 — Fast Query/Home Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(2) Referring to Figure 26, enter a complete or partial license plate number in the **Plate** field. You can search a partial plate number by typing in a few characters of the plate you want to look up, regardless of where the characters are in the sequence on the plate. If you are doing a partial plate search then make sure to check ON the Contains option. In this example, plate “EMA4856” is used. When you are finished typing in the **Plate** field, click **Search**.



□ Contains

EMA4856

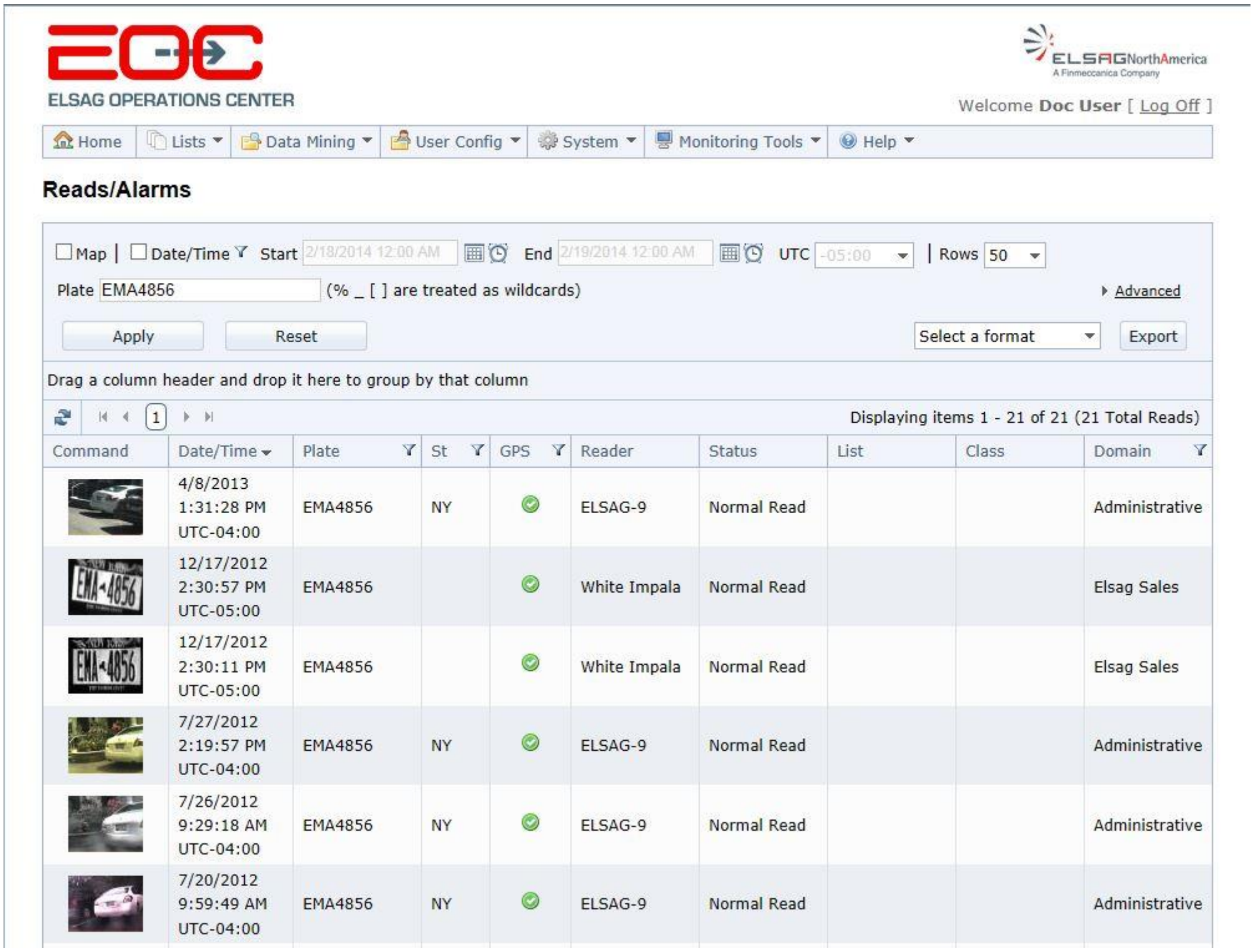
EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:45 PM UTC-05:00

Figure 26 — Fast Query Character Search

(3) You can also use wildcards to expand your search.

- **%** substitutes for any character zero or more times in this position
- **_** means a single character in this position
- **[ ]** means any one of the characters inside the brackets in the position
- For example:
  - ABC% finds all plates of any length starting with ABC
  - %123 finds all plates of any length ending in 123
  - A%3 finds all plates of any length starting with A and ending with 3
  - A__1234 finds all plates beginning with A, followed by any 2 characters, followed by 1234, and
  - A[B8]1234 finds only two plates (AB1234 and A81234).

(4) Referring to Figure 27, the EOC will then display all the results that match the **Plate** field, allowing you to select the one you want to examine more closely.



Welcome **Doc User** [Log Off]

Reads/Alarms

□ Map | □ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate EMA4856 (% _ [ ] are treated as wildcards)

Select a format

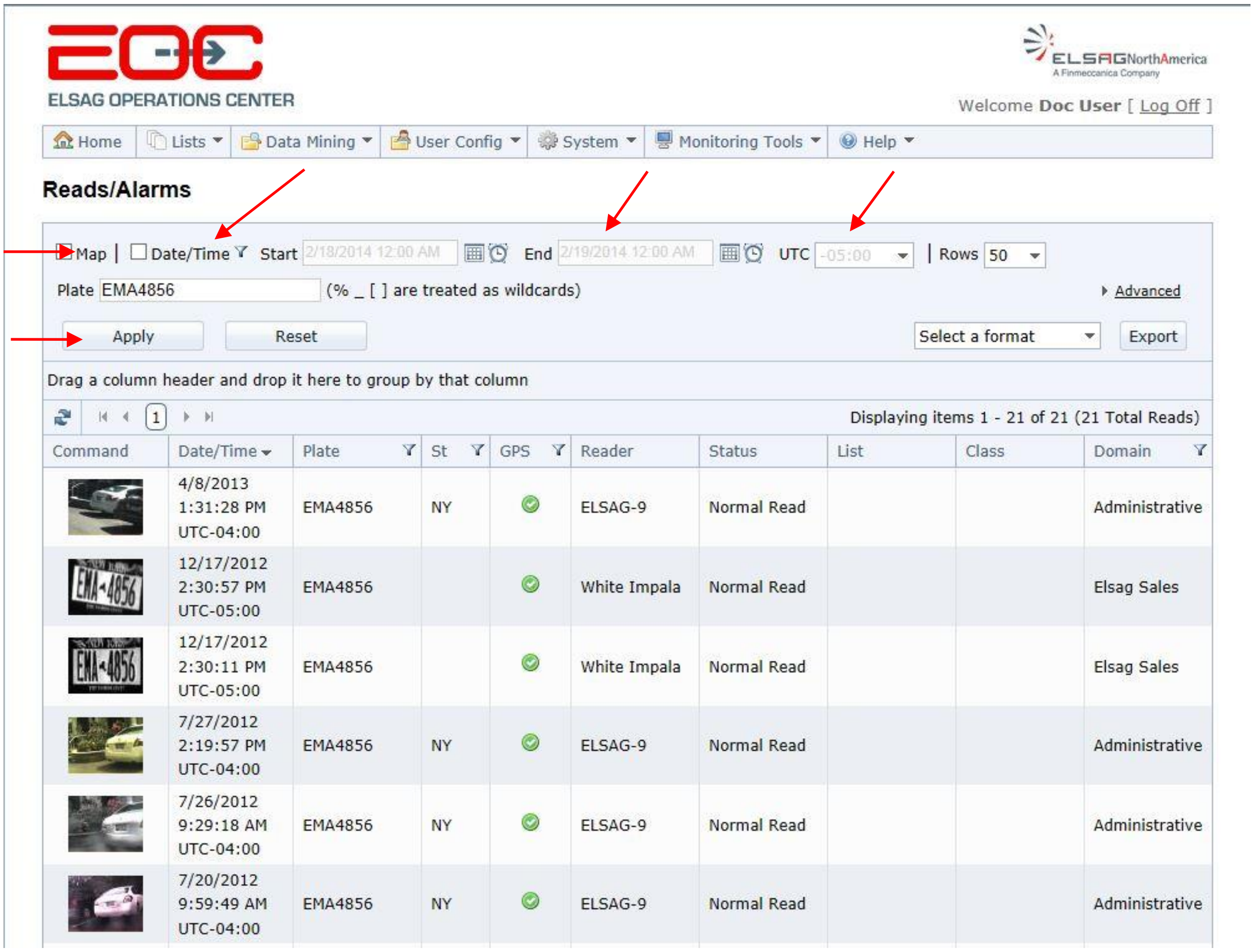
Drag a column header and drop it here to group by that column

1 Displaying items 1 - 21 of 21 (21 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	4/8/2013 1:31:28 PM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	12/17/2012 2:30:57 PM UTC-05:00	EMA4856		✓	White Impala	Normal Read			Elsag Sales
	12/17/2012 2:30:11 PM UTC-05:00	EMA4856		✓	White Impala	Normal Read			Elsag Sales
	7/27/2012 2:19:57 PM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	7/26/2012 9:29:18 AM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	7/20/2012 9:59:49 AM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 27 — Fast Query Results Page

(5) On this page as shown in Figure 28, you can now filter your results using the **Date/Time** filter. Select **Date/Time** filter first and then enter the **Start Date** and **End Date** you are interested in checking. When finished, click **Apply**.



Welcome Doc User [Log Off]

Reads/Alarms

☑ Map | ☐ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate EMA4856 (% _ [ ] are treated as wildcards)

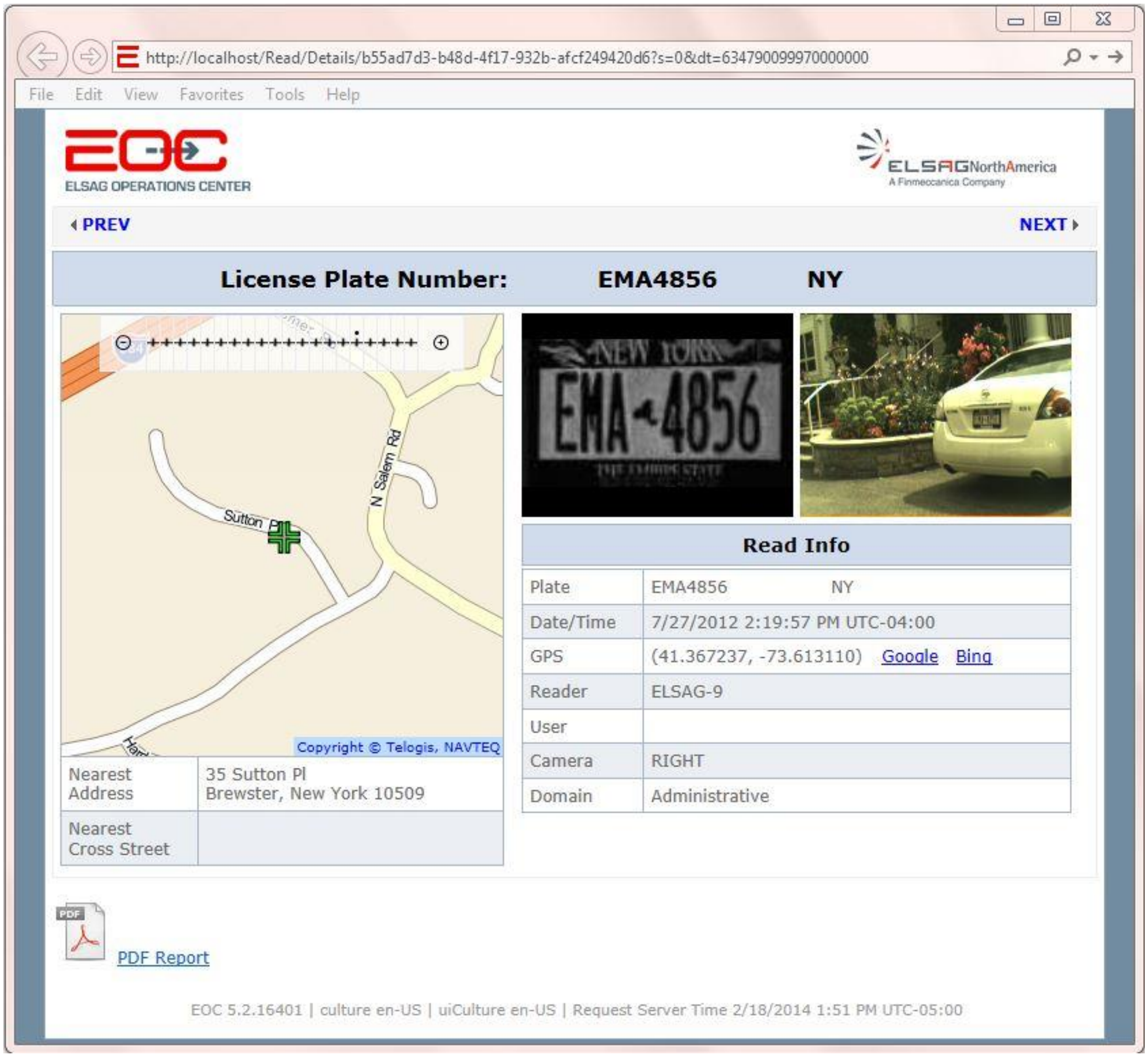
Drag a column header and drop it here to group by that column

Displaying items 1 - 21 of 21 (21 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	4/8/2013 1:31:28 PM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	12/17/2012 2:30:57 PM UTC-05:00	EMA4856		✓	White Impala	Normal Read			Elsag Sales
	12/17/2012 2:30:11 PM UTC-05:00	EMA4856		✓	White Impala	Normal Read			Elsag Sales
	7/27/2012 2:19:57 PM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	7/26/2012 9:29:18 AM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	7/20/2012 9:59:49 AM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 28 — Query Reads Parameters

(6) Referring to Figure 29, you can also view a specific read's details by selecting the image itself, located under the **Command** column. This will show you a read's information and enlarge the plate/vehicle image. In the lower left corner, there is a PDF icon. The PDF file contains the camera images for the read as well as the detailed results images. You can click to open the file and save it to a location outside the EOC.


http://localhost/Read/Details/b55ad7d3-b48d-4f17-932b-afcf249420d6?s=0&dt=634790099970000000
File Edit View Favorites Tools Help
EOC
ELSAG OPERATIONS CENTER
ELSAG NorthAmerica
A Finmeccanica Company
PREV
NEXT
N Salem Rd
Sutton Pl
Copyright © Telogis, NAVTEQ
PDF

License Plate Number: EMA4856 NY

Nearest Address	35 Sutton Pl Brewster, New York 10509
Nearest Cross Street	

Read Info

Plate	EMA4856 NY
Date/Time	7/27/2012 2:19:57 PM UTC-04:00
GPS	(41.367237, -73.613110) Google Bing
Reader	ELSAG-9
User	
Camera	RIGHT
Domain	Administrative

PDF Report

EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:51 PM UTC-05:00

Figure 29 — Fast Query Image Detail

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

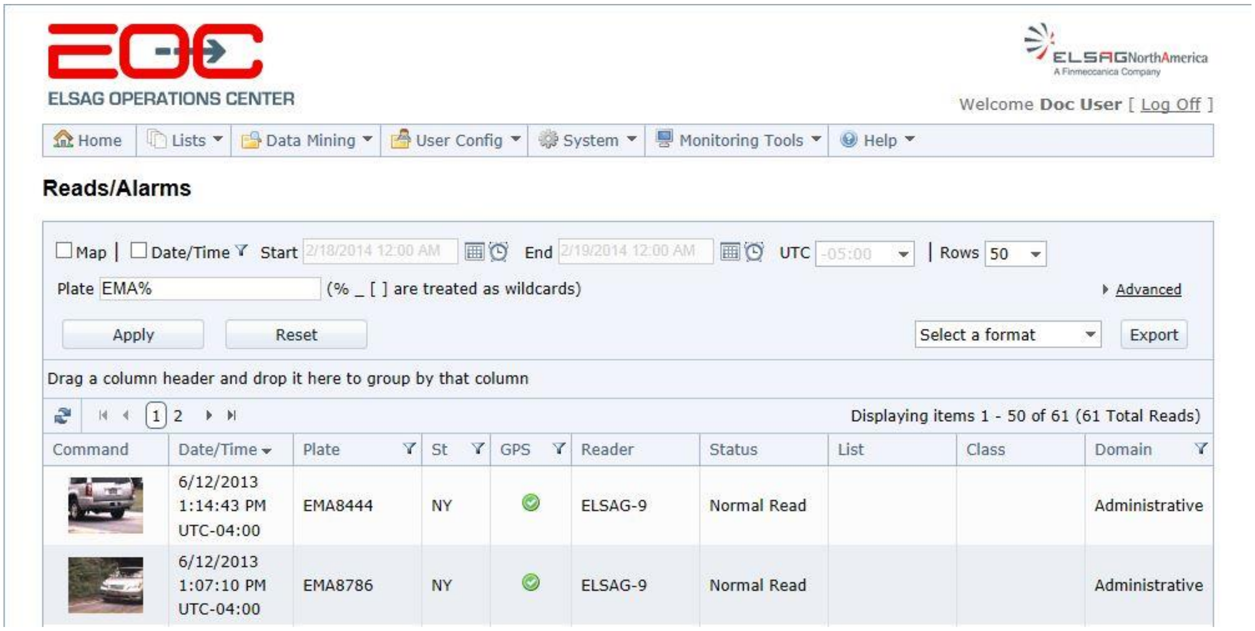
Query Reads

To do more sophisticated searches, refer to Figure 30 and use the basic query functionality of EOC.

(1) To begin searching the data in the EOC database, select **Data Mining > Query Reads**. You'll see the beginning of the list of all reads in the database.

(2) Enter a plate number in the **Plate** field. You can use wildcards as in fast search to help aid your search. If reference is needed refer to Step 2 in **Fast Query**.

(3) Press **Apply**. (**Reset** sets the default filters and page view; **Export CSV** lets you export the search results to a csv file without images; **Export HTML** lets you export the search results to an HTML file with images, **Export PDF** lets you export the search results to an HTML file with images as individual PDF reports.



Reads/Alarms

□ Map | □ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate EMA% (% _ [ ] are treated as wildcards)

Select a format

Drag a column header and drop it here to group by that column

1 2 Displaying items 1 - 50 of 61 (61 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	6/12/2013 1:14:43 PM UTC-04:00	EMA8444	NY	✓	ELSAG-9	Normal Read			Administrative
	6/12/2013 1:07:10 PM UTC-04:00	EMA8786	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 30 — Basic Query Results Screen

(4) You can filter the results as described in the sections below.

Filtering Results

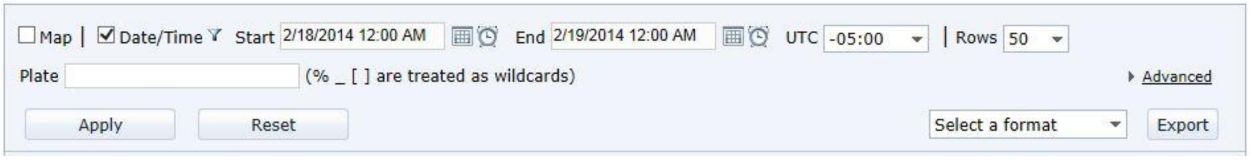
Because the mechanism of filtering the data is substantially the same regardless of what you're filtering on, the sections below demonstrate only the most common procedures for filtering by date and time and by plate number and state. You can use the filters on all attribute columns to structure complex queries, however. Use the general principles explained in the procedure below to filter on other attributes.

Note that filters are cumulative. For example, if you filter first by plate number, then by state, your final result set will contain only those plate numbers from the first search that also come from the state(s) you filtered by.

❑ Filtering by a Default Twenty-Four Hour Period

To filter by a 24-hour period, use the following steps:

(1) Referring to Figure 31, select the **Date/Time Filter** checkbox. (Notice that the date and time in the **Start** and **End** text boxes are no longer grayed out.)



□ Map | ☑ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate (% _ [ ] are treated as wildcards)

Figure 31 — Date/Time Filter Enabled for Default Period

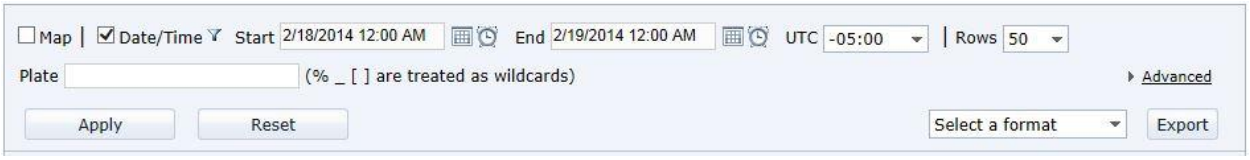
(2) Press the **Apply** button.

NOTE: The set of reads displayed is narrowed to reads made during the 24-hour period. The default period begins at midnight yesterday and ends at midnight today.

❑ Filtering by any Date and Time Interval

To filter by any date and time interval, perform the following steps:

(1) Referring to Figure 32, select the **Date/Time Filter** checkbox. (Notice that the date and time in the **Start** and **End** text boxes are no longer grayed out.)

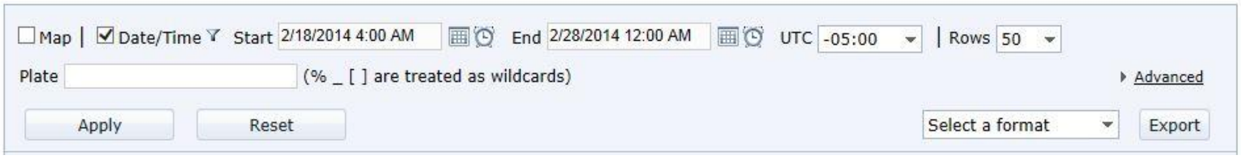


□ Map | ☑ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate (% _ [ ] are treated as wildcards)

Figure 32 — Date/Time Filter Enabled

(2) Referring to Figure 33, use the small calendar and clock icons to set the **Start** and **End** of the date interval you want to search.



□ Map | ☑ Date/Time Start 2/18/2014 4:00 AM End 2/28/2014 12:00 AM UTC -05:00 | Rows 50

Plate (% _ [ ] are treated as wildcards)

Figure 33 — Date/Time Filter Set to Non-Default Interval

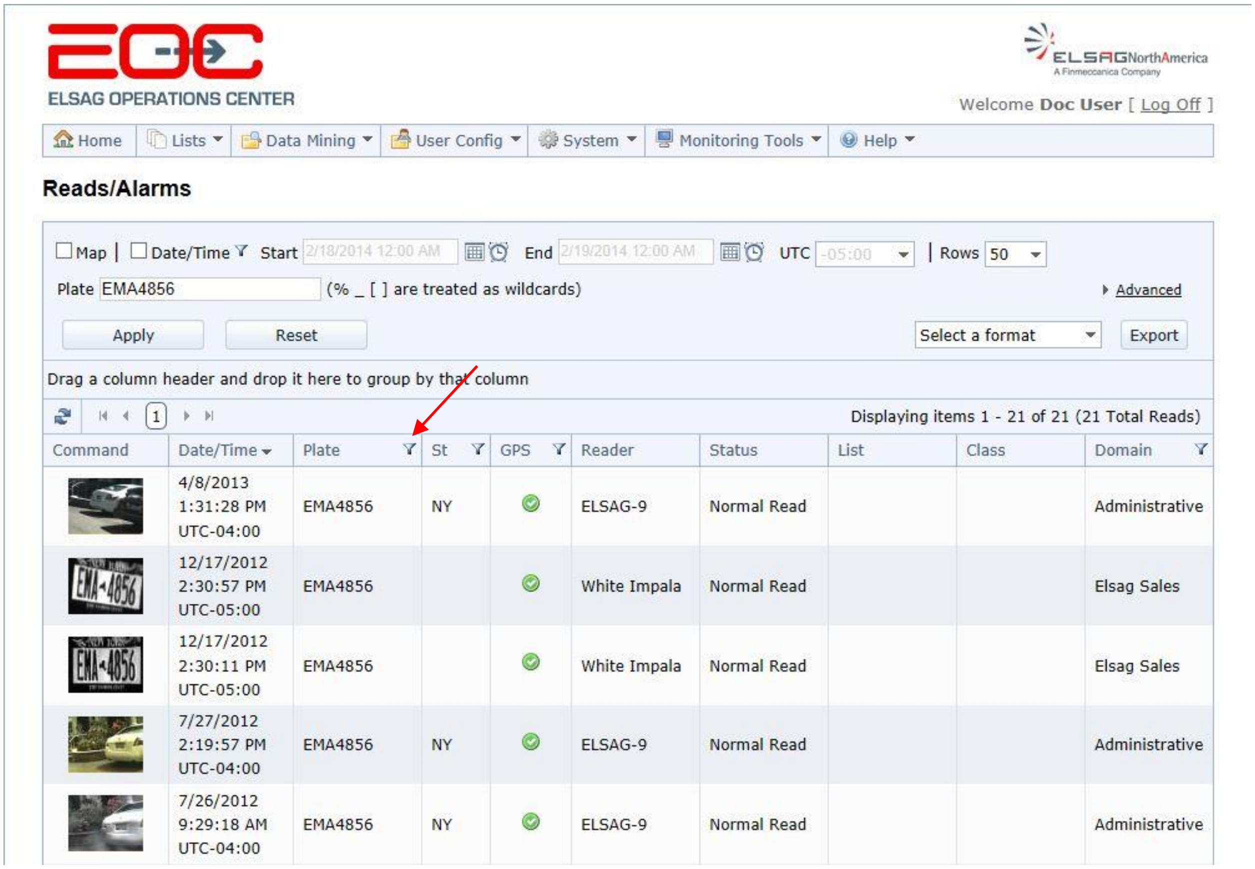
(3) Press the **Apply** button. The set of reads displayed is narrowed to reads made during the specified date and time interval.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

❑ Filtering by Plate Number and State

A common search allows you to filter the plate data by plate number and state. This allows you to inspect the activity of a single plate or a small group of plates over a period of time. To filter the plate read data by plate number and state perform the following steps:

(1) Referring to Figure 34, press the ▽ (Filter Icon) in the **Plate** column.



Reads/Alarms

☐ Map | ☐ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate EMA4856 (% _ [ ] are treated as wildcards)

Advanced

Apply Reset Select a format Export

Drag a column header and drop it here to group by that column

Displaying items 1 - 21 of 21 (21 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	4/8/2013 1:31:28 PM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	12/17/2012 2:30:57 PM UTC-05:00	EMA4856		✓	White Impala	Normal Read			Elsag Sales
	12/17/2012 2:30:11 PM UTC-05:00	EMA4856		✓	White Impala	Normal Read			Elsag Sales
	7/27/2012 2:19:57 PM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative
	7/26/2012 9:29:18 AM UTC-04:00	EMA4856	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 34 — Plate Filter Icon

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(2) The image shown in Figure 35 will appear.

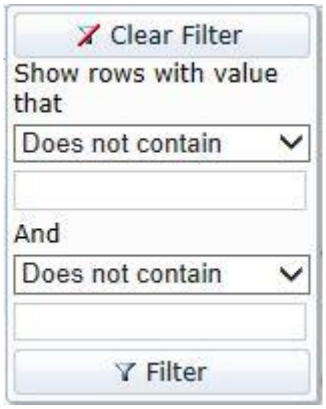
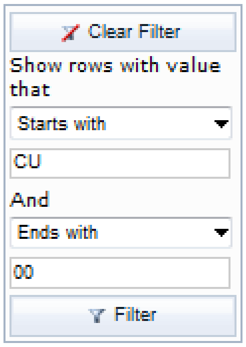


Figure 35 — Plate Search Filter

(3) Referring to Figure 36, use the dropdowns and textboxes to bind the search for plates that interest you. For example, the search below looks for plates that begin with the characters **CU** and ends with **00**.

NOTE: You can undo a filter action by pressing the **Clear Filter** button at the top of the filter panel.



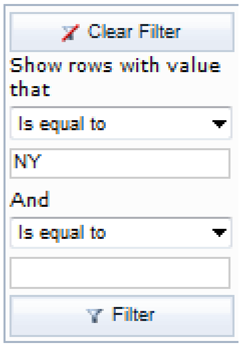
Show rows with value that
Starts with
CU
And
Ends with
00

Figure 36 — Plate Search Filter Filled-in

(4) Press the **Filter** button at the bottom of the panel and the display will change to show only plates with the specified characteristics.

NOTE: You can undo a filter action by pressing the **Clear Filter** button at the top of the filter panel.

(5) Referring to Figure 37, now do the same thing in the **State** column to select a state.



Show rows with value that

Is equal to

NY

And

Is equal to

Figure 37 — State Search Filter Filled-in

(6) Press the **Filter** button at the bottom of the panel and the display will change to show only plates with the previously specified characteristics that are also from **NY** State.

NOTE: You can undo a filter action by pressing the **Clear Filter** button at the top of the filter panel.

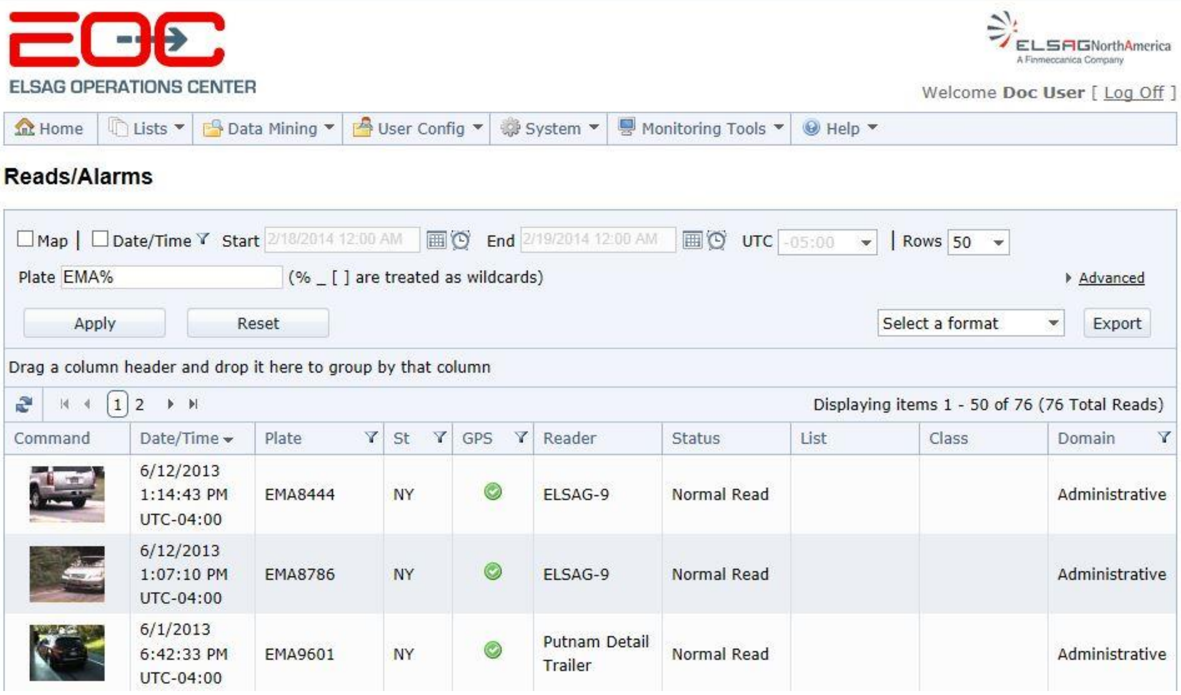
❑ Filtering by Other Attributes

Columns with filter icons can be filtered. When you filter by other attributes, the effect is additive. For example, filtering on *Is Equal to* **CT** in the **State** list and *Ends with* **00** in the **Plate** list will give you a list of all Connecticut plates that end in 00.

❑ Change Column Display

You can group the display by a specific data attribute of the reads by dragging the column header to the area indicated on the display. For example: to group the displayed reads by plate number. To change the column display, perform the following steps:

(1) Create the set of read data you need (see Figure 38).



Welcome Doc User [Log Off]

Reads/Alarms

□ Map | □ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate EMA% (% _ [ ] are treated as wildcards)

Select a format

Drag a column header and drop it here to group by that column

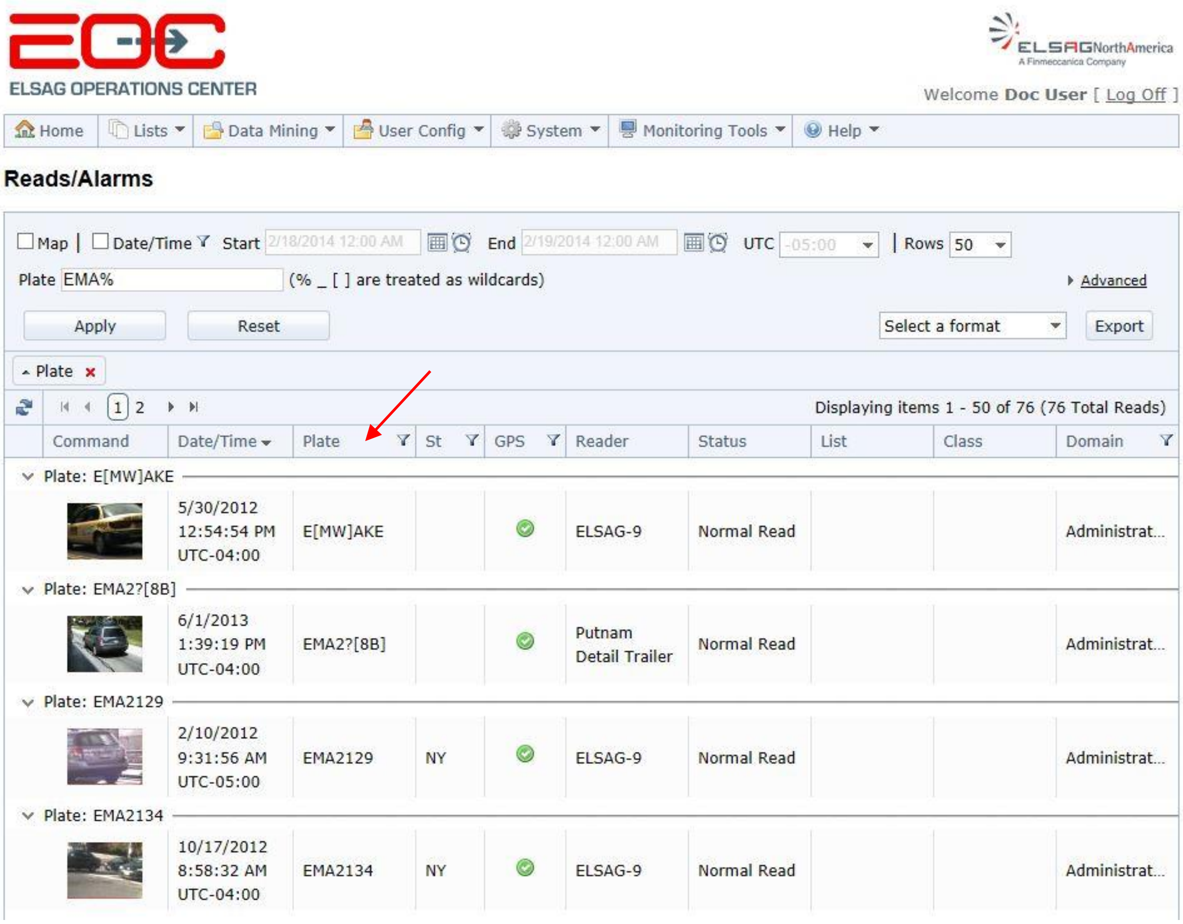
1 2 Displaying items 1 - 50 of 76 (76 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	6/12/2013 1:14:43 PM UTC-04:00	EMA8444	NY	✓	ELSAG-9	Normal Read			Administrative
	6/12/2013 1:07:10 PM UTC-04:00	EMA8786	NY	✓	ELSAG-9	Normal Read			Administrative
	6/1/2013 6:42:33 PM UTC-04:00	EMA9601	NY	✓	Putnam Detail Trailer	Normal Read			Administrative

Figure 38 — Read Data Set before Column Grouping

(2) Referring to Figure 39, drag the Plate column header to the specified area. Notice that the read data has been reorganized to display by plate number.

NOTE: To cancel the grouping click on the red “X.”



Welcome Doc User [Log Off]

Reads/Alarms

□ Map | □ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate EMA% (% _ [ ] are treated as wildcards) Advanced

Displaying items 1 - 50 of 76 (76 Total Reads)

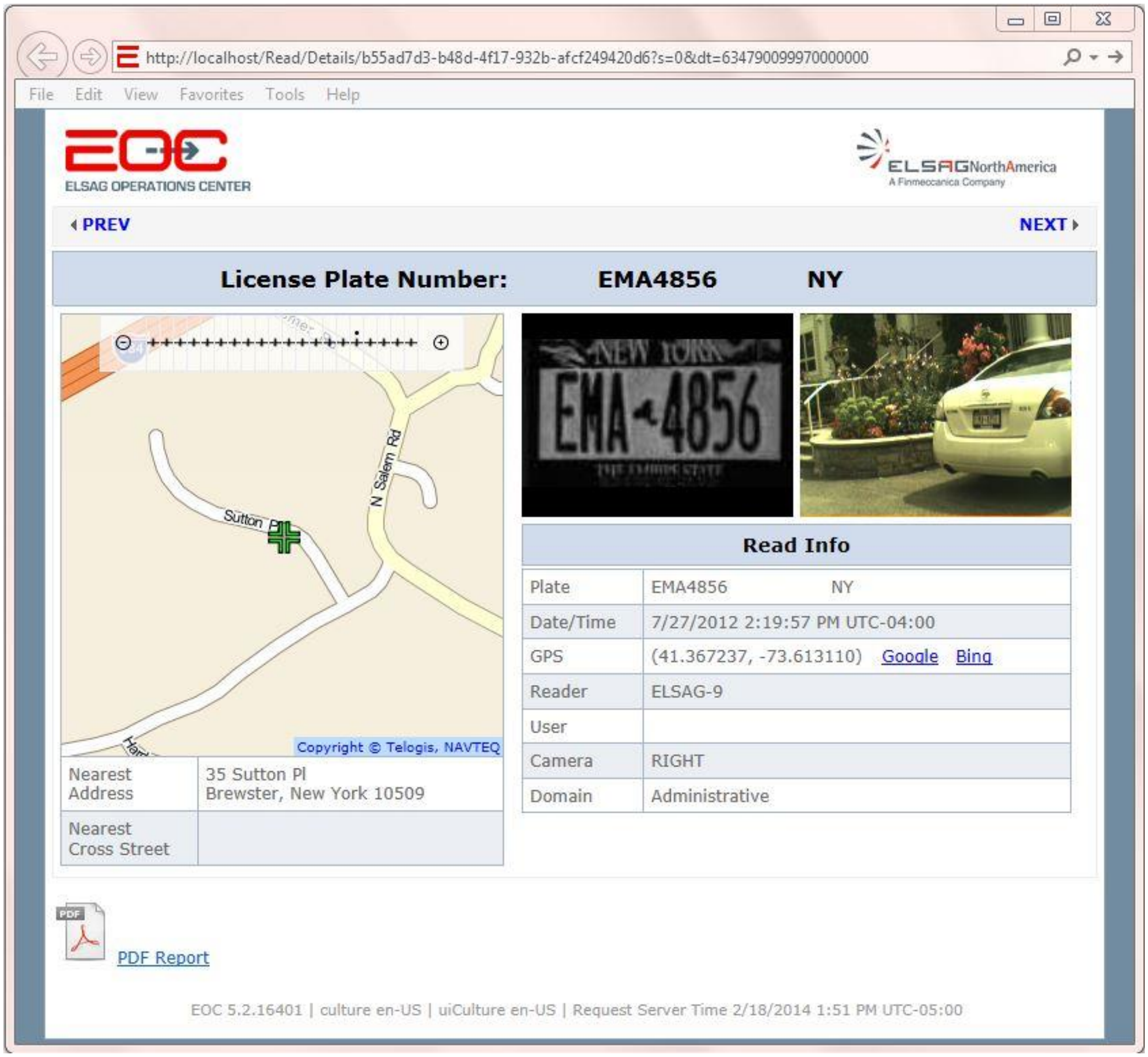
Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
Plate: E[MW]AKE									
	5/30/2012 12:54:54 PM UTC-04:00	E[MW]AKE		✓	ELSAG-9	Normal Read			Administrat...
Plate: EMA2?[8B]									
	6/1/2013 1:39:19 PM UTC-04:00	EMA2?[8B]		✓	Putnam Detail Trailer	Normal Read			Administrat...
Plate: EMA2129									
	2/10/2012 9:31:56 AM UTC-05:00	EMA2129	NY	✓	ELSAG-9	Normal Read			Administrat...
Plate: EMA2134									
	10/17/2012 8:58:32 AM UTC-04:00	EMA2134	NY	✓	ELSAG-9	Normal Read			Administrat...

Figure 39 — Read Data Set after Column Grouping

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

❑ **Viewing Plate Read Images**

(3) To view the picture associated with a plate read, click on the picture.



http://localhost/Read/Details/b55ad7d3-b48d-4f17-932b-afcf249420d6?s=0&dt=634790099970000000
File Edit View Favorites Tools Help
EOC
ELSAG OPERATIONS CENTER
ELSAG NorthAmerica
A Finmeccanica Company
◂ PREV
NEXT ▸
Sutton Pl
N Salem Rd
Copyright © Telogis, NAVTEQ
NEW YORK
EMA-4856
PDF Report

License Plate Number: EMA4856 NY

Nearest Address	35 Sutton Pl Brewster, New York 10509
Nearest Cross Street	

Read Info

Plate	EMA4856 NY
Date/Time	7/27/2012 2:19:57 PM UTC-04:00
GPS	(41.367237, -73.613110) Google Bing
Reader	ELSAG-9
User	
Camera	RIGHT
Domain	Administrative

EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 1:51 PM UTC-05:00

Figure 40 — Plate Read Image

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(4) Referring to Figure 41, click on the full vehicle image and use the **Brighten** and **Sharpen** buttons to refine it. (Use **Restore** to undo changes.)

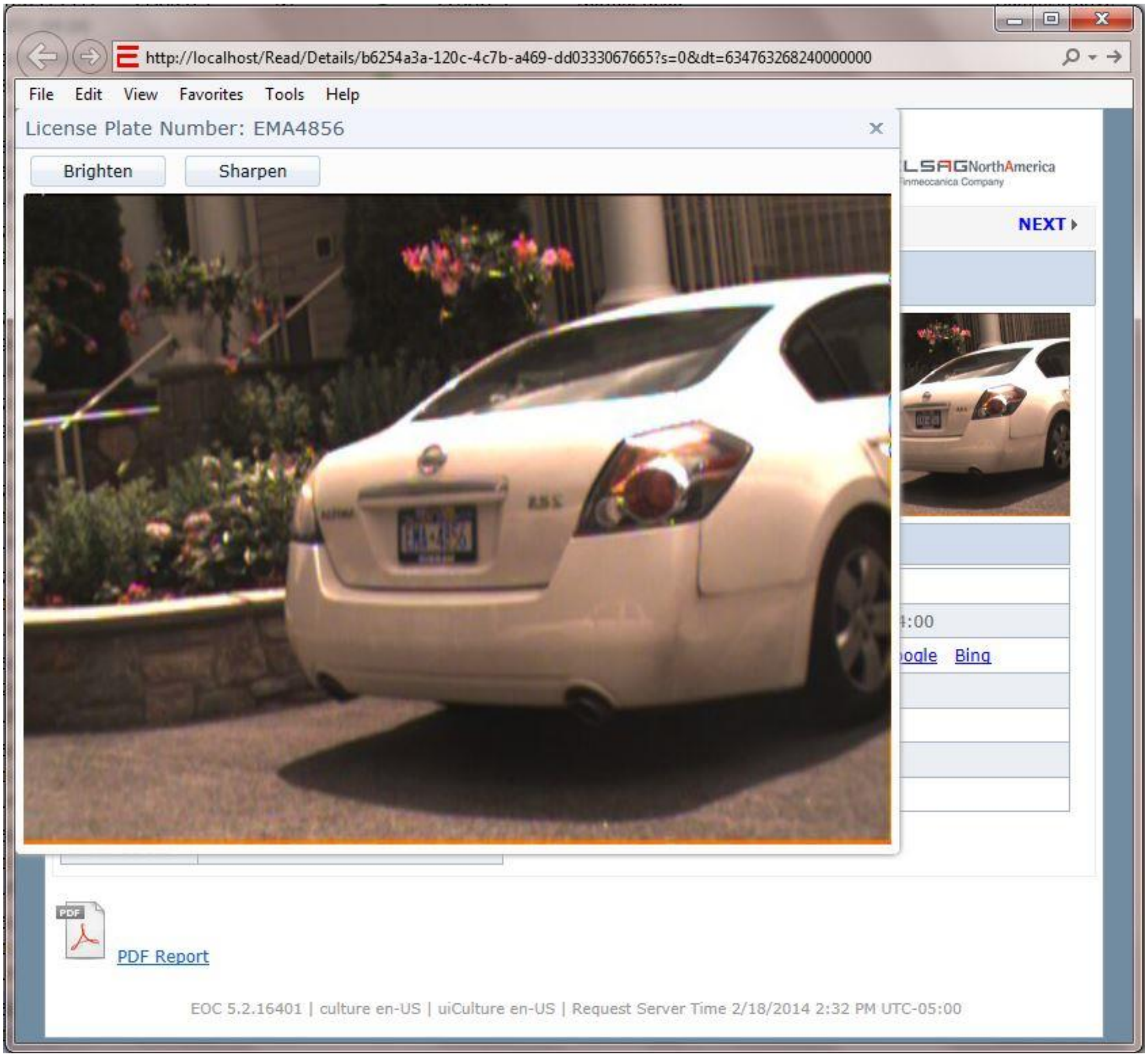

http://localhost/Read/Details/b6254a3a-120c-4c7b-a469-dd0333067665?s=0&dt=634763268240000000
File Edit View Favorites Tools Help
License Plate Number: EMA4856
Brighten
Sharpen
NEXT
4:00
oogle Bing
PDF Report
EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 2:32 PM UTC-05:00

Figure 41 — Plate Read Color Image Close-up

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(5) Referring to Figure 42, click on the plate image to see the black and white plate only.

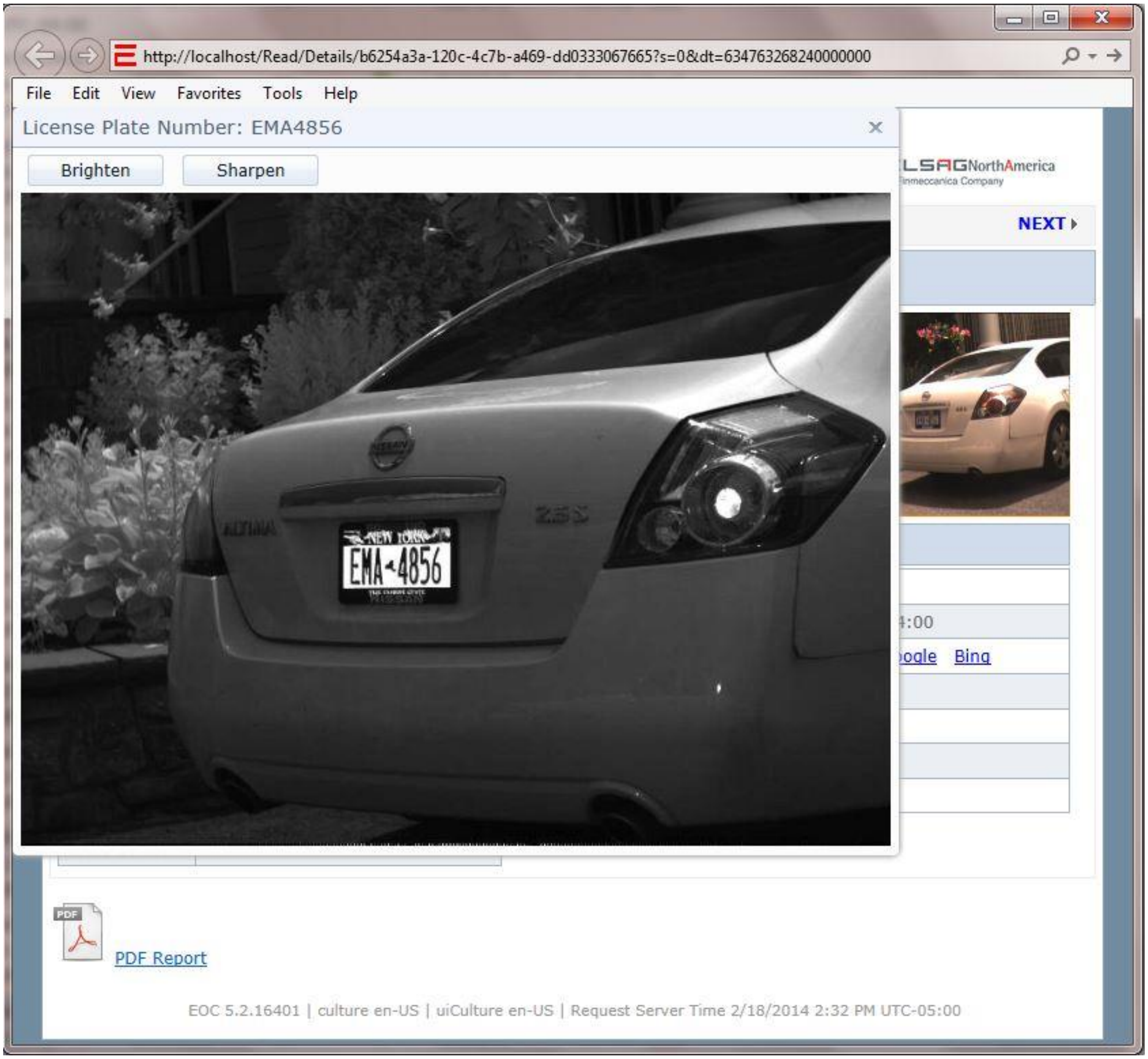

http://localhost/Read/Details/b6254a3a-120c-4c7b-a469-dd0333067665?s=0&dt=634763268240000000
File Edit View Favorites Tools Help
License Plate Number: EMA4856
Brighten
Sharpen
NEW YORK
EMA-4856
ELSAG North America
NEXT
:00
oogle Bing
PDF Report
EOC 5.2.16401 | culture en-US | uiCulture en-US | Request Server Time 2/18/2014 2:32 PM UTC-05:00

Figure 42 — Plate Read B&W Image Close-up

(6) Assuming you have more than one plate read in your result set, you can page through the images and information using the Previous/Next arrows at the top of the page as shown Figure 43.

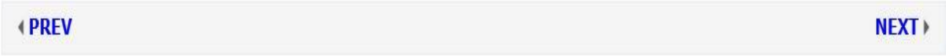


Figure 43 — Plate Read Navigation

You can also use keyboard shortcuts — Left/Right arrow keys to navigate the reads in the data set.

Querying Functions

❑ Apply Button

Use the **Apply** button to apply changes you make to these elements in the read screen header:

- Start date and time (when Date/Time Filter is checked)
- End date and time (when Date/Time Filter is checked)
- UTC (Time Zone Offset), and
- Rows (number of rows of reads shown per displayed page).

❑ Export Button

- Use the **Export dropdown** to select CSV (comma-separated values) file, HTML or PDF.

  NOTE: Exporting to PDF is similar to exporting to HTML but images are in the PDF format similar to the Query Details page PDF.

❑ Reset Button

- Use the **Reset** button to undo all the changes you have made to any data fields in the display.

❑ Filtering the Query List

In order to narrow the set of plate read data in the database, you can filter the query list by one or more of the following:

- Date and time of plate reads (You can also query for all the reads in a particular time period.)
- Plate number
- State
- Latitude and Longitude of read location, and
- Domain of read data.

❑ Advanced

Click the **Advanced** link to further filter a search or result set by:

- Readers (Cameras)
- Remote Servers
- Alarm Status
- Lists, and
- Alarm Classes.

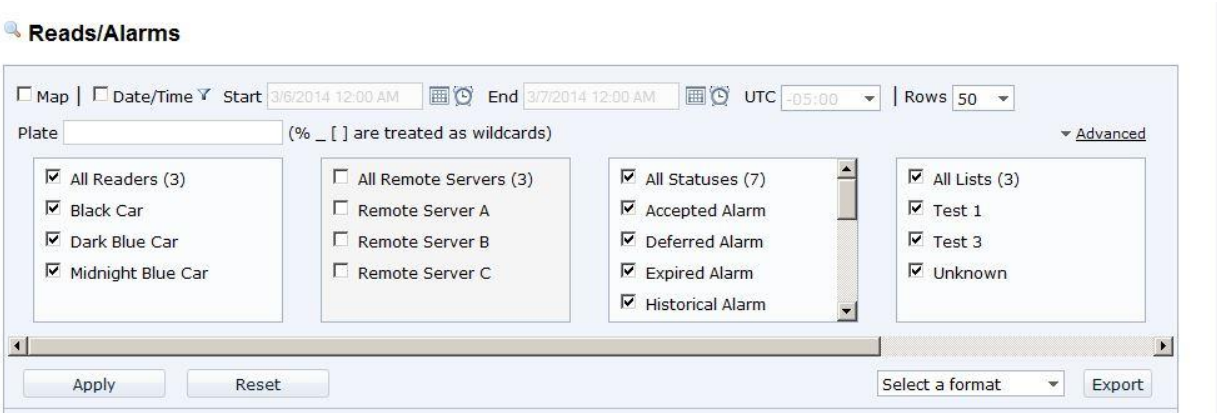
Querying Across Multiple EOC Implementations

You can query plate reads and alarms across multiple implementations of the EOC, assuming your system has been configured to connect to the servers of those EOCs. Your access to other EOC servers will be controlled by your permissions on that server.

To make a query search multiple EOC databases, refer to Figure 44 and perform the following steps:

(1) Select **Data Mining > Query Reads**.

(2) Select **Advanced**. If your implementation is correctly configured and you have permissions, you’ll see a list of the remote servers you can access.



Reads/Alarms

□ Map | □ Date/Time Start 3/6/2014 12:00 AM End 3/7/2014 12:00 AM UTC -05:00 | Rows 50

Plate (% _ [ ] are treated as wildcards)

☑ All Readers (3)
☑ Black Car
☑ Dark Blue Car
☑ Midnight Blue Car

□ All Remote Servers (3)
□ Remote Server A
□ Remote Server B
□ Remote Server C

☑ All Statuses (7)
☑ Accepted Alarm
☑ Deferred Alarm
☑ Expired Alarm
☑ Historical Alarm

☑ All Lists (3)
☑ Test 1
☑ Test 3
☑ Unknown

Figure 44 — EOC Remote Servers

(3) Select each remote EOC server you want to query by checking the box next to it. To query all remote servers, check the **All Remote Servers** box.

NOTE: Data from the local EOC server is represented by the **Readers** pane.

- To query data in the local EOC as well as data from remote EOC servers, leave some or all of the boxes in the **Readers** pane checked.
- If you only want to search the remote EOC servers, uncheck all the boxes in the **Readers** pane.

(4) Select **Apply**.

(5) Perform your search as normal.

NOTE: You can refine your search in the same way as a local server search, by individual readers, statuses and/or alarm classes.

(6) Your results will include all plate reads and/or alarms found in all the servers you selected.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

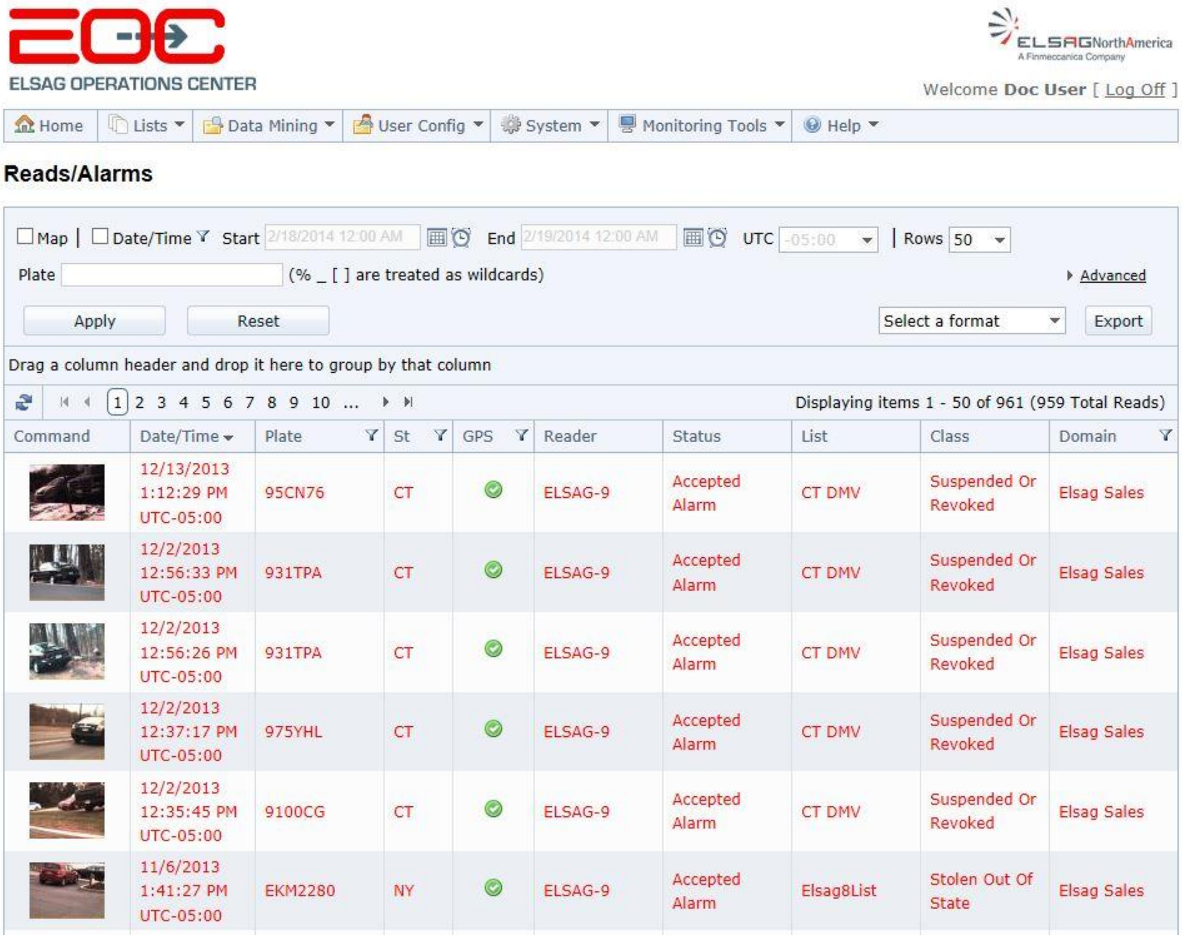
Searching for Alarms

You search alarms in the EOC database using the same mechanisms that you use to search for plates.

Referring to Figure 45, to begin searching the alarms in the EOC database, select **Data Mining > View Alarms**. You will see the beginning of the list of all alarms in the database.

> **NOTE:** Alarm information is displayed in red. From here, you can perform all the same operations on the alarm data as you did on the plate read data.

You can customize your alarm search by selecting **Advanced** and selecting a specific **Alarm Status** or **Alarm Class**.



Reads/Alarms

□ Map | □ Date/Time Start 2/18/2014 12:00 AM End 2/19/2014 12:00 AM UTC -05:00 | Rows 50

Plate (% _ [ ] are treated as wildcards)

Drag a column header and drop it here to group by that column

1 2 3 4 5 6 7 8 9 10 ...

Displaying items 1 - 50 of 961 (959 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	12/13/2013 1:12:29 PM UTC-05:00	95CN76	CT	✓	ELSAG-9	Accepted Alarm	CT DMV	Suspended Or Revoked	Elsag Sales
	12/2/2013 12:56:33 PM UTC-05:00	931TPA	CT	✓	ELSAG-9	Accepted Alarm	CT DMV	Suspended Or Revoked	Elsag Sales
	12/2/2013 12:56:26 PM UTC-05:00	931TPA	CT	✓	ELSAG-9	Accepted Alarm	CT DMV	Suspended Or Revoked	Elsag Sales
	12/2/2013 12:37:17 PM UTC-05:00	975YHL	CT	✓	ELSAG-9	Accepted Alarm	CT DMV	Suspended Or Revoked	Elsag Sales
	12/2/2013 12:35:45 PM UTC-05:00	9100CG	CT	✓	ELSAG-9	Accepted Alarm	CT DMV	Suspended Or Revoked	Elsag Sales
	11/6/2013 1:41:27 PM UTC-05:00	EKM2280	NY	✓	ELSAG-9	Accepted Alarm	Elsag8List	Stolen Out Of State	Elsag Sales

Figure 45 — Initial Alarms Screen

❑ Alarm Statuses

When you are viewing alarms, you can sort or group them by the following statuses.

- Pending Alarm — An alarm that awaits operator acceptance or rejection. If the CarSystem application is **not** running and no operator takes action on the alarm, the alarm remains as a Pending Alarm forever.

- Expired Alarm — CarSystem application must be running and a Pending alarm is **not** acted upon by an operator within 2.5 minutes.
- Accepted Alarm — An alarm that has been acted upon by an operator and deemed accurate.
- Rejected Alarm — An alarm that has been rejected by the operator for a number of reasons, including a misread plate, no plate, obsolete List entry or wrong state.
- Deferred Alarm — An alarm that has been deferred for a period of 8 hours. **Ex**: An officer is aware of an alarm but may pass it multiple times while on one shift, so he defers the alert so that the CarSystem Alarm Window does not pop up.
- Historical Alarm — An alarm that is associated with an older read based on an updated List with an entry which has an effective date in the past.

NOTE: Alarms are acted upon by CarSystem operators or EOC users who have permissions for Dispatcher or Alarm Validation Search Results. How to accept, reject or defer Alarms are described in the *MPH-900 CarSystem User's Guide*.

❑ Alarm Classes

The following types of **Alarm Classes** are available for an alarm search:

- Amber/Silver Alert
- Immigration Violator
- Missing Person
- Protection Order
- Scofflaw
- Sexual Offender
- Stolen Out Of State
- Stolen Plate
- Stolen Vehicle
- Supervised Release
- Suspended or Revoked
- Tax Scofflaw
- Unknown
- Violent Gang
- Wanted Person
- While List Alarm, and
- Other.

❑ Alarms and Permissions

As with all data in the EOC system, your access to alarms depends on the permissions you have with respect to the lists from which those alarms are generated.

If you search alarms for a particular plate read and you do not have permissions to the list from which the alarm came, you will not see any alarm for that read.

Cross Search

Cross search allows you to compare the results of multiple queries (up to five) to determine if plate reads are duplicated within a time range or across different time ranges, in the same location or in different locations. Cross search is another way, like convoy search, that you can see patterns in the plate read data.

> **NOTE:** Currently, Cross Search is not configured to work with remote servers. Results returned from a remote server will not be displayed in a Cross Search.

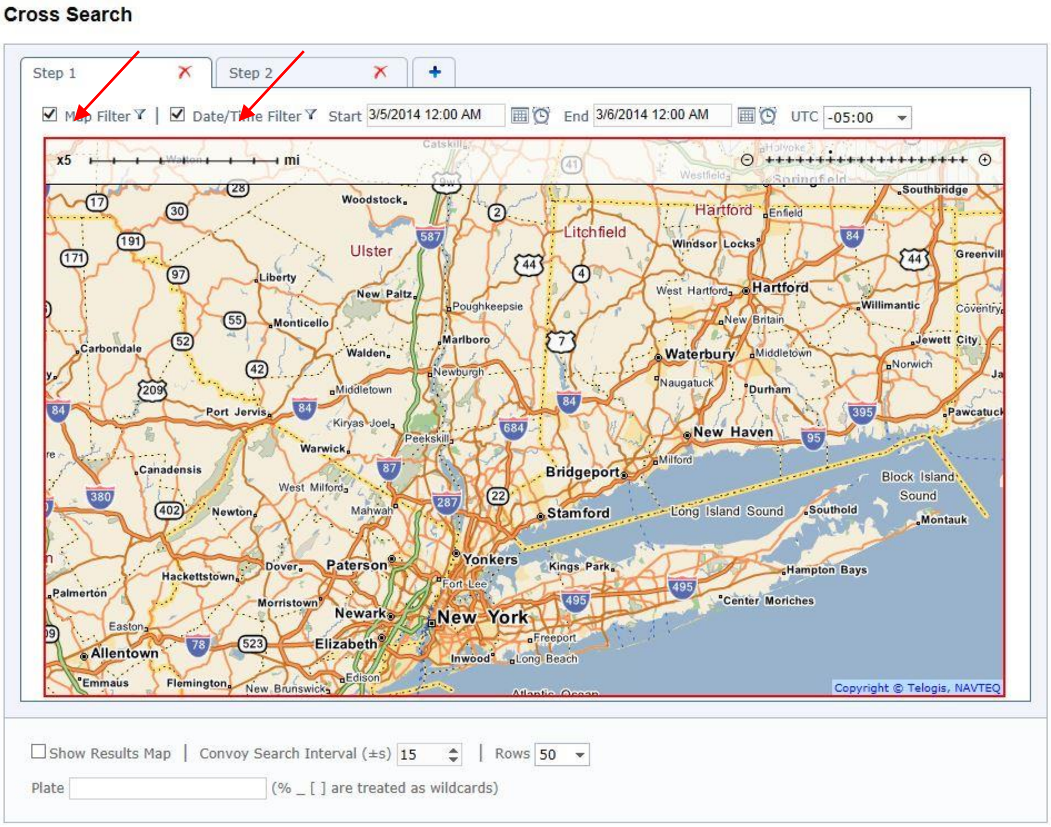
For example, you can use cross search to:

- Determine if one or more vehicles was present at a specific location during a different time frame, and
- Determine if the same vehicle or vehicles was present at different locations during different time frames.

Example of a **Cross Search**: A series of thefts have been occurring throughout neighboring cities. Using time frames specific to these incidents, **Cross Search** can be used to see if a certain vehicle(s) were present in both areas while the crimes took place.

To perform a Cross Search, perform the steps that follow:

(1) Select **Data Mining > Cross Search**. You will see the screen shown Figure 46.



Cross Search

Step 1 ✗ | Step 2 ✗ | +

☑ Map Filter | ☑ Date/Time Filter Start 3/5/2014 12:00 AM End 3/6/2014 12:00 AM UTC -05:00

□ Show Results Map | Convoy Search Interval (±s) 15 | Rows 50

Plate (% _ [ ] are treated as wildcards)

Figure 46 — Cross Search Initial Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(2) Referring to Figure 46, before specifying a plate you can select the search parameters pertinent to your search. These include:

- **Map Filter** — Set the location on the map to search for a vehicle(s), and
- **Date/Time Filter** — Search for a vehicle(s) by choosing a specific time frame.

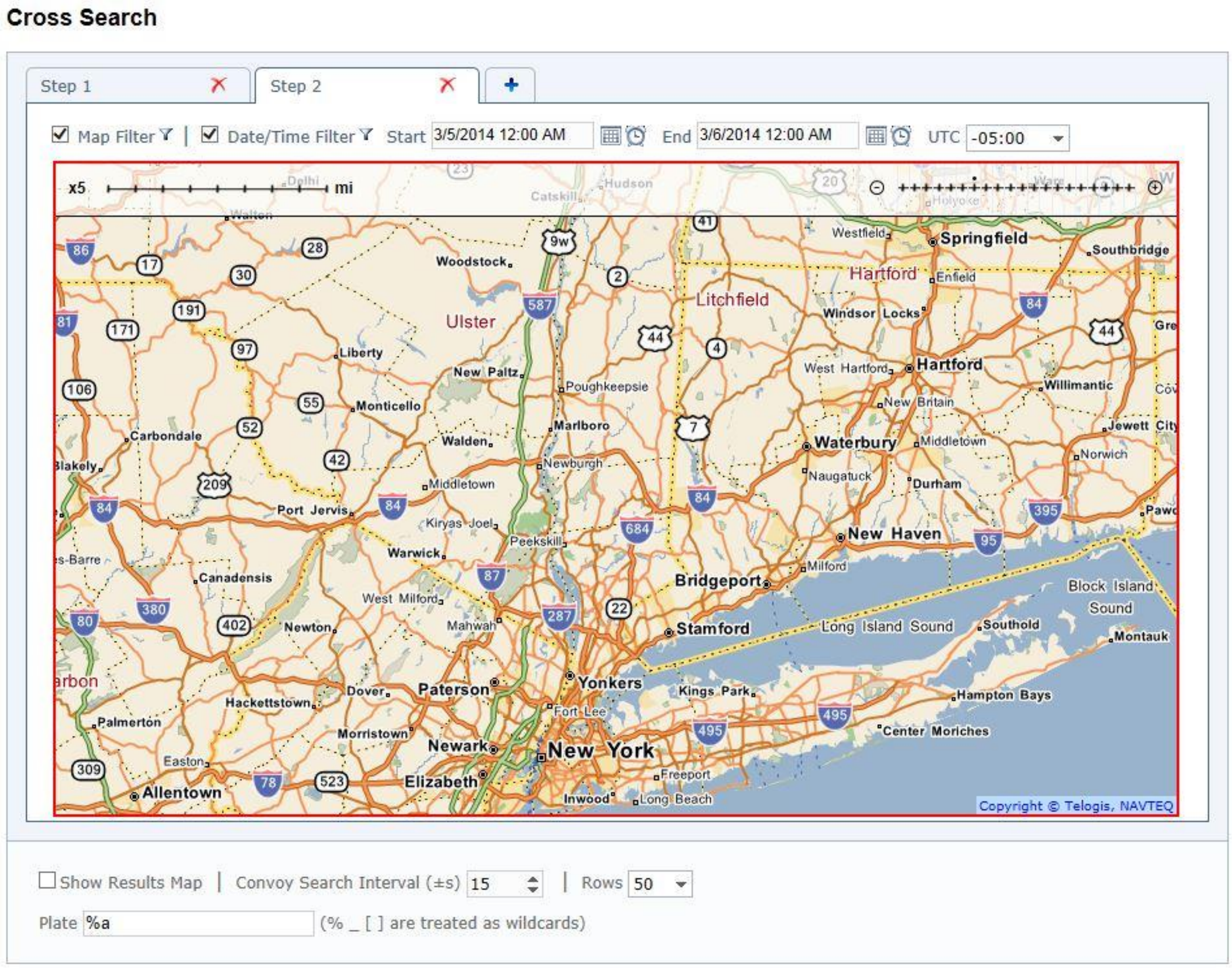
(3) Press the plus sign (+) to add another query to the cross search. To use **Cross Search** you must use a minimum of two queries.

(4) Once you have a minimum of two queries you can search for the plate you are interested in by entering its characters in the **Plate** search, which can be found on the lower left hand side of the screen.

(5) You can add additional queries (up to five total) as you did above. If you want to delete a query, click on the X (queries you made after that one will move to the left). For example, if you wanted to see if the plate you searched for above was also at another location, create a new pane and search with a different location.

(6) Referring to Figure 47, you can also check the **Show results map** checkbox (and press **Apply**) to display the search results on the map and use the usual map manipulation tools (zoom, etc.) to make the display meaningful.

NOTE: When you have finished a cross search, you can reproduce the same results at any time. Save the final results page URL as a Favorite or Bookmark so that you can run the same report by clicking on the Favorite. That address will bring you back to the results.



Cross Search

Step 1 ✗ | Step 2 ✗ | +

☑ Map Filter | ☑ Date/Time Filter Start 3/5/2014 12:00 AM End 3/6/2014 12:00 AM UTC -05:00

□ Show Results Map | Convoy Search Interval (±s) 15 | Rows 50

Plate %a (% _ [ ] are treated as wildcards)

Figure 47 — Cross Search Additional Query

Using Maps

The EOC includes a cartography function that allows you to display plate reads and/or alarms on a map to show where the reads or alarms occurred. This is useful management and reporting information that you can also export to other forms for later use.

The map function is enabled by checking the **Map** checkbox. However, since the map display is driven by the data you select from the database, you must first narrow your search to plates and/or alarms of interest.

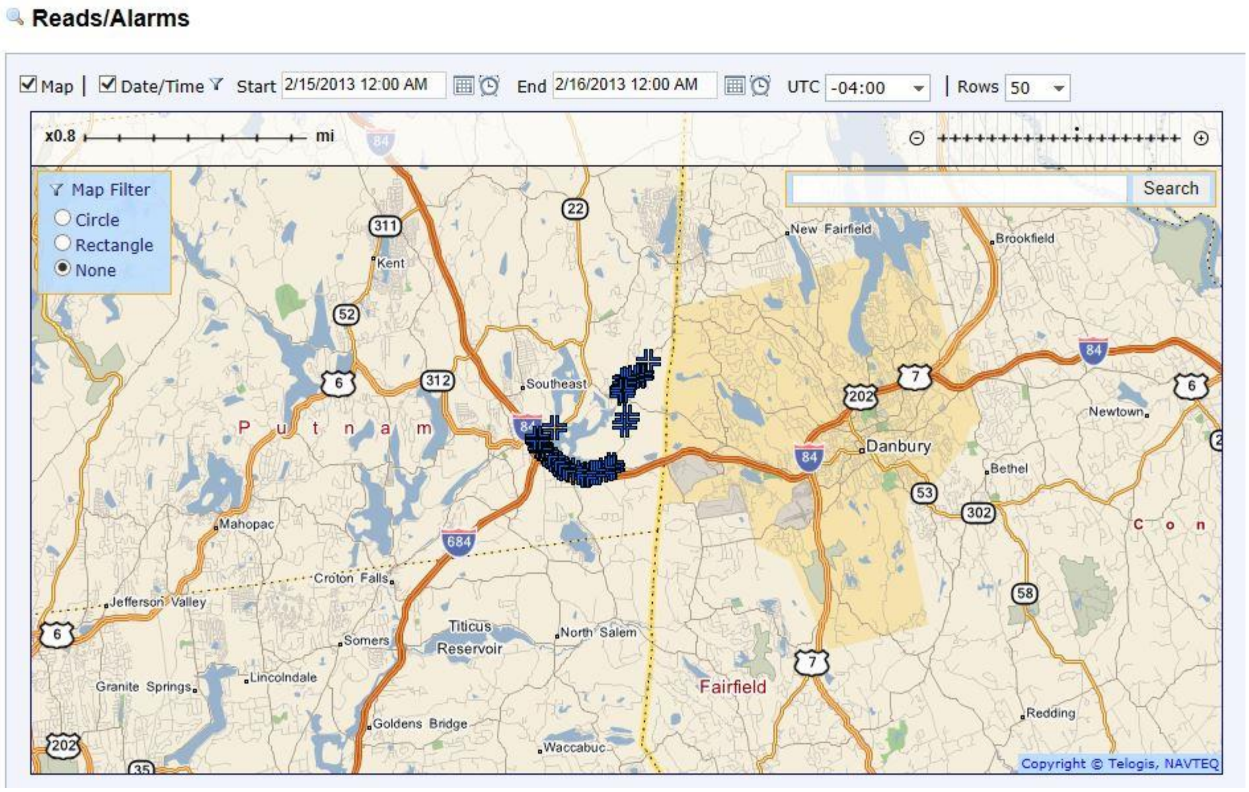
Essentially, using maps is a two-step process:

- Set boundaries on the data you're interested in using filters: Start and End Time, Plate number, State, etc., and
- Select the **Map** checkbox and use the Map interface to accomplish the tasks you need.

The Map UI

❑ Map Checkbox

The **Map Checkbox** is how you enable the mapping function on any data set that you have chosen. After you select the group of plate and/or alarm data that you're interested in, select the **Map Checkbox** to display a map with the points illustrated on it.



Reads/Alarms

☑ Map | ☑ Date/Time Start 2/15/2013 12:00 AM End 2/16/2013 12:00 AM UTC -04:00 | Rows 50

Map Filter
○ Circle
○ Rectangle
● None

Figure 48 — Initial Map Read Showing Data Points

❑ Changing the Display

As you can see, many of the selected points overlap and obscure each other on the map. The mapping user interface allows you to widen the display so that the points are discrete and more easily viewed. Use the zoom slider in the upper right hand corner of the display (see Figure 49) to zoom in or out on the display.

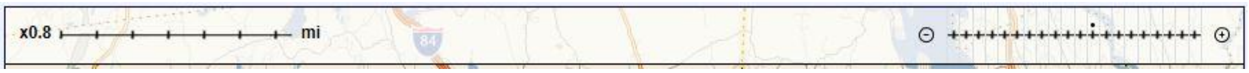
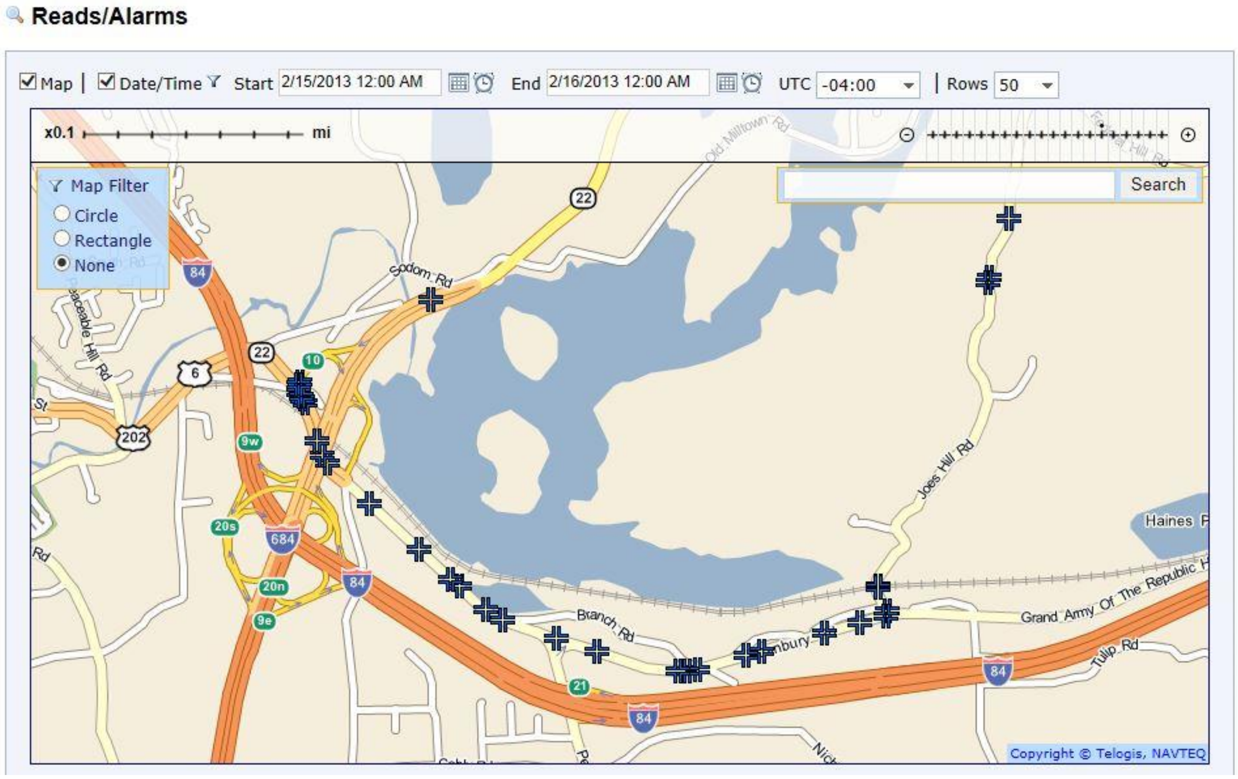


Figure 49 — Slider

Referring to Figure 50, click toward the right (toward the + sign) to zoom in on the map, or increase the magnification. Moving to the left decreases the magnification. The left and center tracks report the magnification in miles and kilometers.

NOTE In the magnified map below that the data points are much easier to distinguish.



Reads/Alarms

☑ Map | ☑ Date/Time Start 2/15/2013 12:00 AM End 2/16/2013 12:00 AM UTC -04:00 | Rows 50

Map Filter

○ Circle

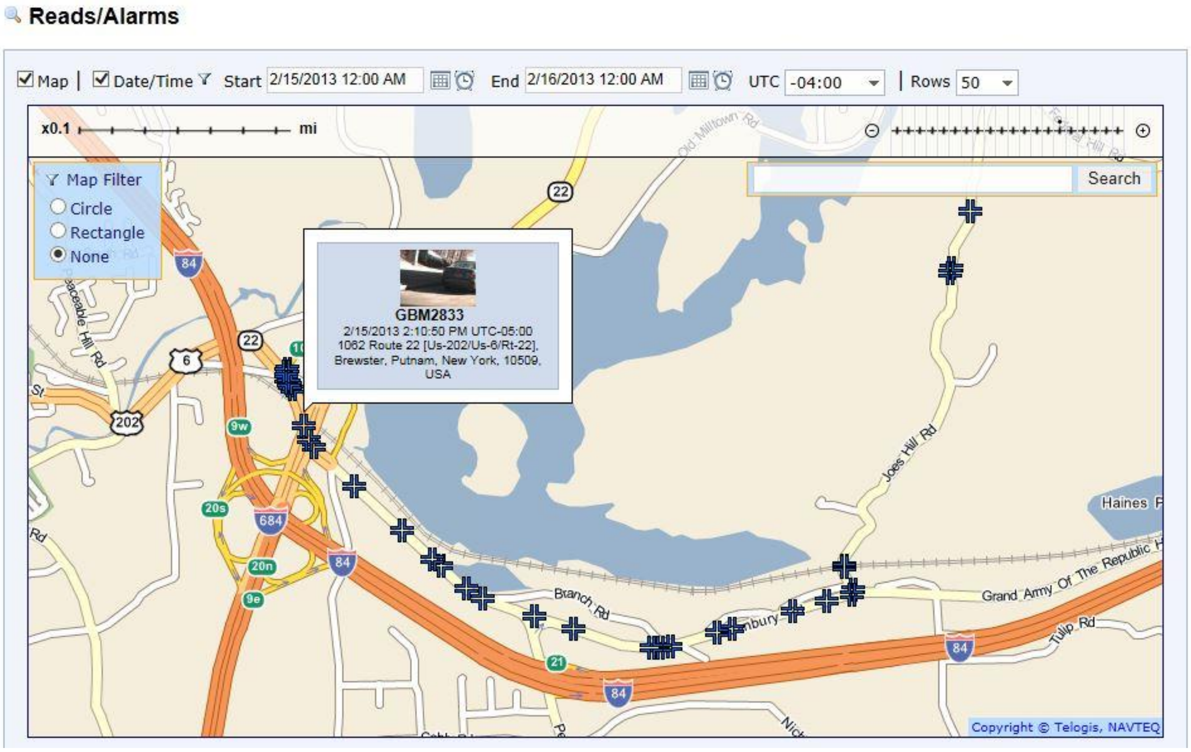
○ Rectangle

● None

Figure 50 — Magnified Map

- **Finding a Point’s Address**

Referring to Figure 51, you can find out the address of a particular read by hovering your cursor over the point.



Reads/Alarms

☑ Map | ☑ Date/Time Start 2/15/2013 12:00 AM End 2/16/2013 12:00 AM UTC -04:00 | Rows 50

Map Filter
○ Circle
○ Rectangle
● None

Search

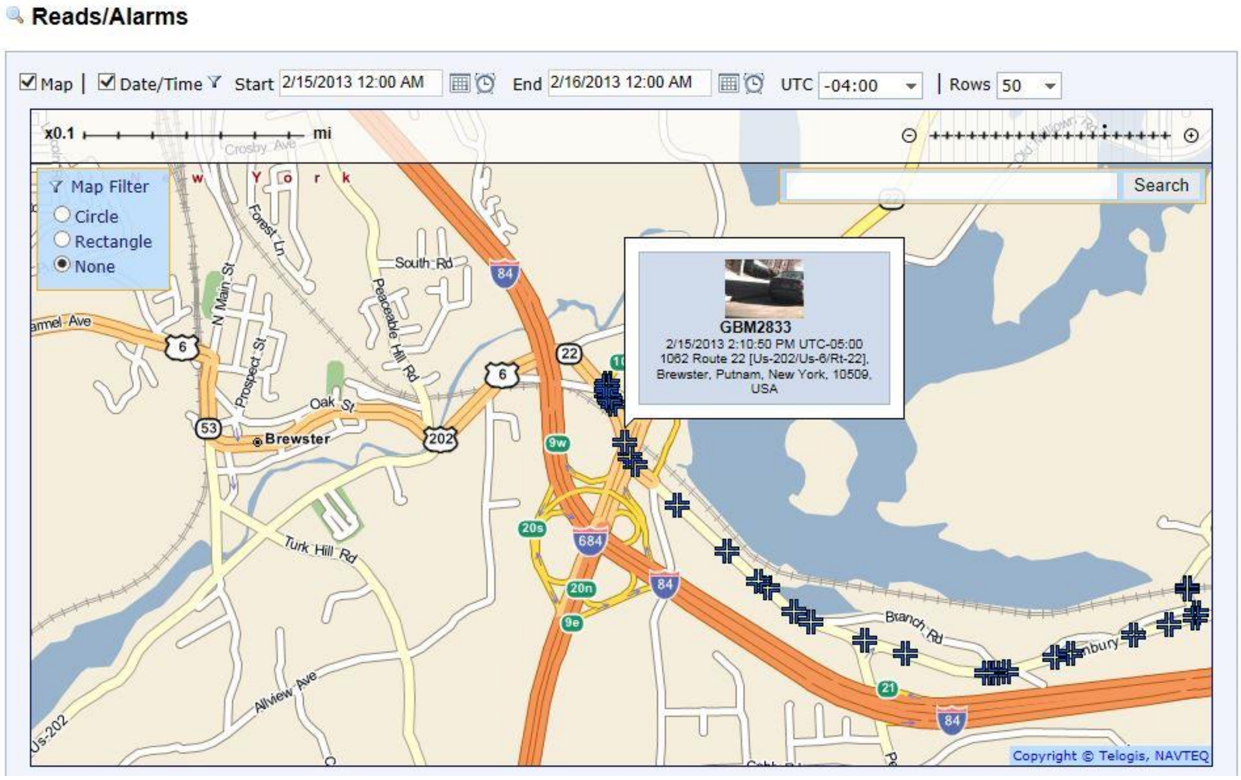
GBM2833
2/15/2013 2:10:50 PM UTC-05:00
1062 Route 22 [Us-202/Us-6/Rt-22],
Brewster, Putnam, New York, 10509,
USA

Figure 51 — Selected Area Address Highlighted

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

❑ Center on a Point

Referring to Figure 52, you can also center the map on a particular point by double clicking on the point.



Reads/Alarms

☑ Map | ☑ Date/Time Start 2/15/2013 12:00 AM End 2/16/2013 12:00 AM UTC -04:00 | Rows 50

Map Filter
○ Circle
○ Rectangle
● None

GBM2833
2/15/2013 2:10:50 PM UTC-05:00
1062 Route 22 [Us-202/Us-6/Rt-22],
Brewster, Putnam, New York, 10509,
USA

Figure 52 — Map Centered on a Point

❑ Move Map Display

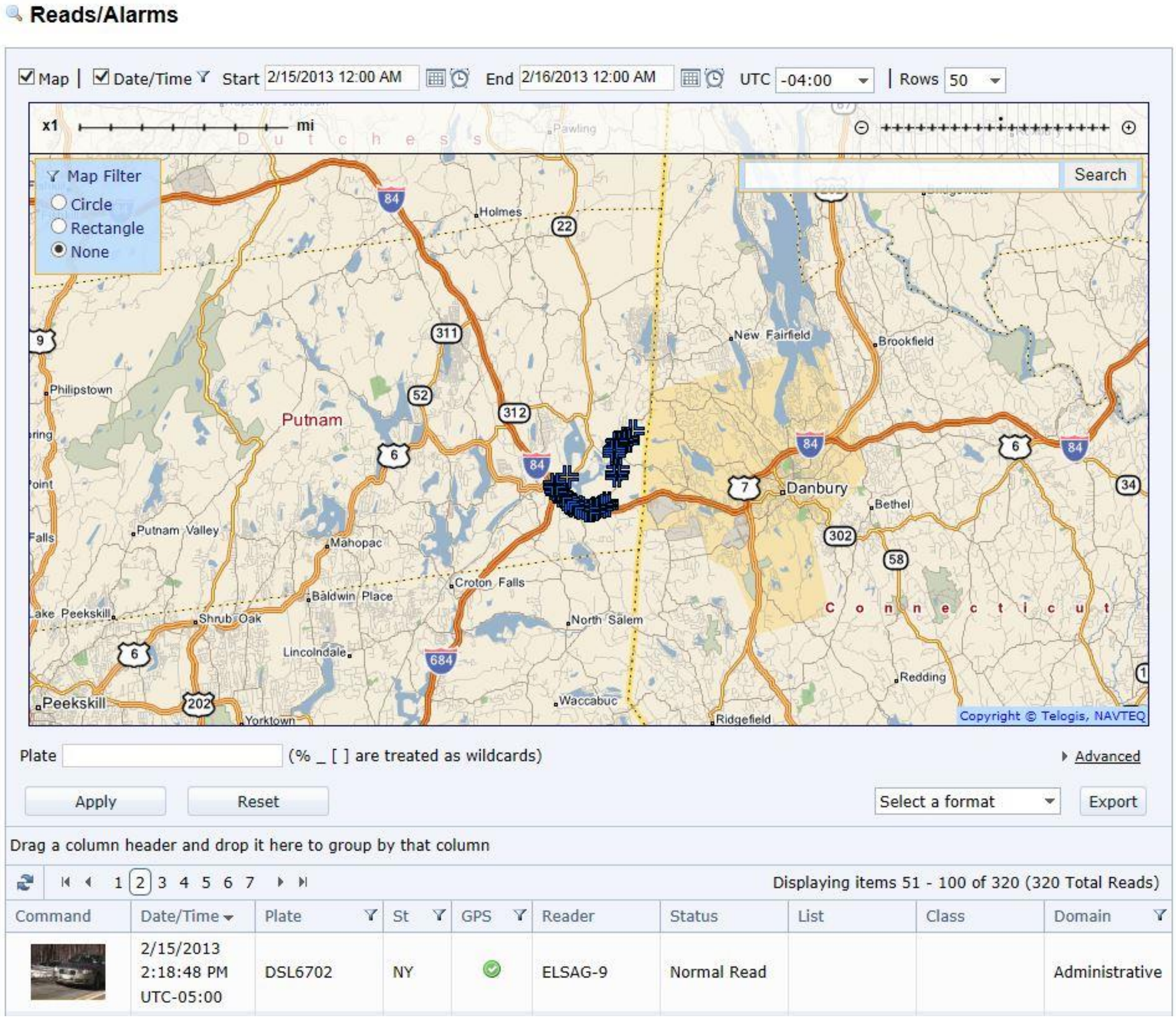
You can move the map display by clicking the left mouse button while the cursor is inside the map and using the small hand cursor to move the map display in any direction.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

❑ Enable Map Filter

Referring to Figure 53, you use the **Enable Map Filter** to focus on those data points that are within the section of the map you have visible. A map filter can be shaped as a circle or rectangle. The following sample screens demonstrate.

The first screen shows some of the data points you selected. Note that the list of reads below the map includes 320 items, though not all are visible.



Reads/Alarms

☑ Map | ☑ Date/Time Start 2/15/2013 12:00 AM End 2/16/2013 12:00 AM UTC -04:00 | Rows 50

Map Filter
○ Circle
○ Rectangle
● None

Plate (% _ [ ] are treated as wildcards) Advanced

Apply Reset Select a format Export

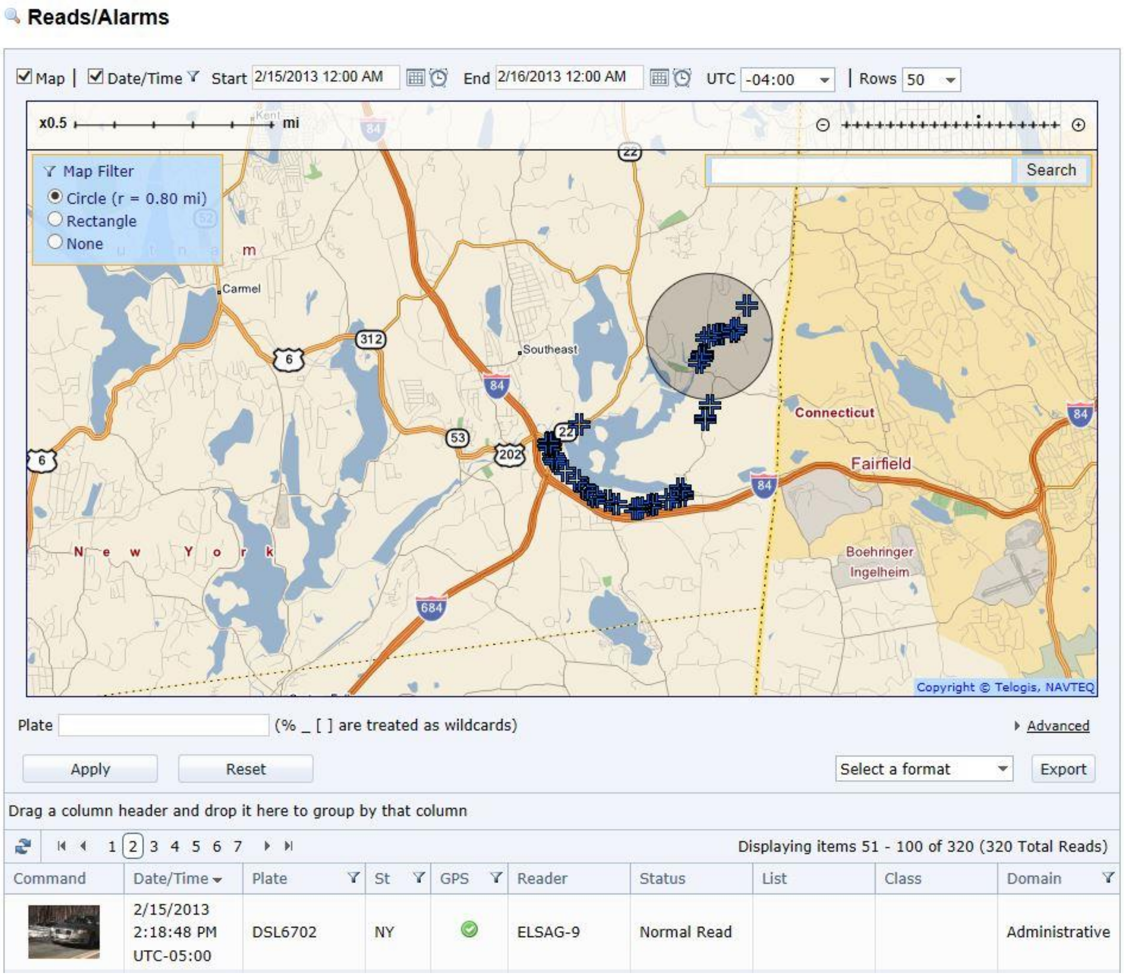
Drag a column header and drop it here to group by that column

1 2 3 4 5 6 7 Displaying items 51 - 100 of 320 (320 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	2/15/2013 2:18:48 PM UTC-05:00	DSL6702	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 53 — Display Before Enabling Map Filter

Referring to Figure 54, select the **Map Filter Circle** or **Rectangle** radio button options. Position your mouse over the map where you want to create the filter. While holding the Right mouse button down move the mouse to create the filter area on the map.



Reads/Alarms

☑ Map | ☑ Date/Time Start 2/15/2013 12:00 AM End 2/16/2013 12:00 AM UTC -04:00 | Rows 50

Map Filter
● Circle (r = 0.80 mi)
○ Rectangle
○ None

Plate (% _ [ ] are treated as wildcards)

Drag a column header and drop it here to group by that column

1 2 3 4 5 6 7 Displaying items 51 - 100 of 320 (320 Total Reads)

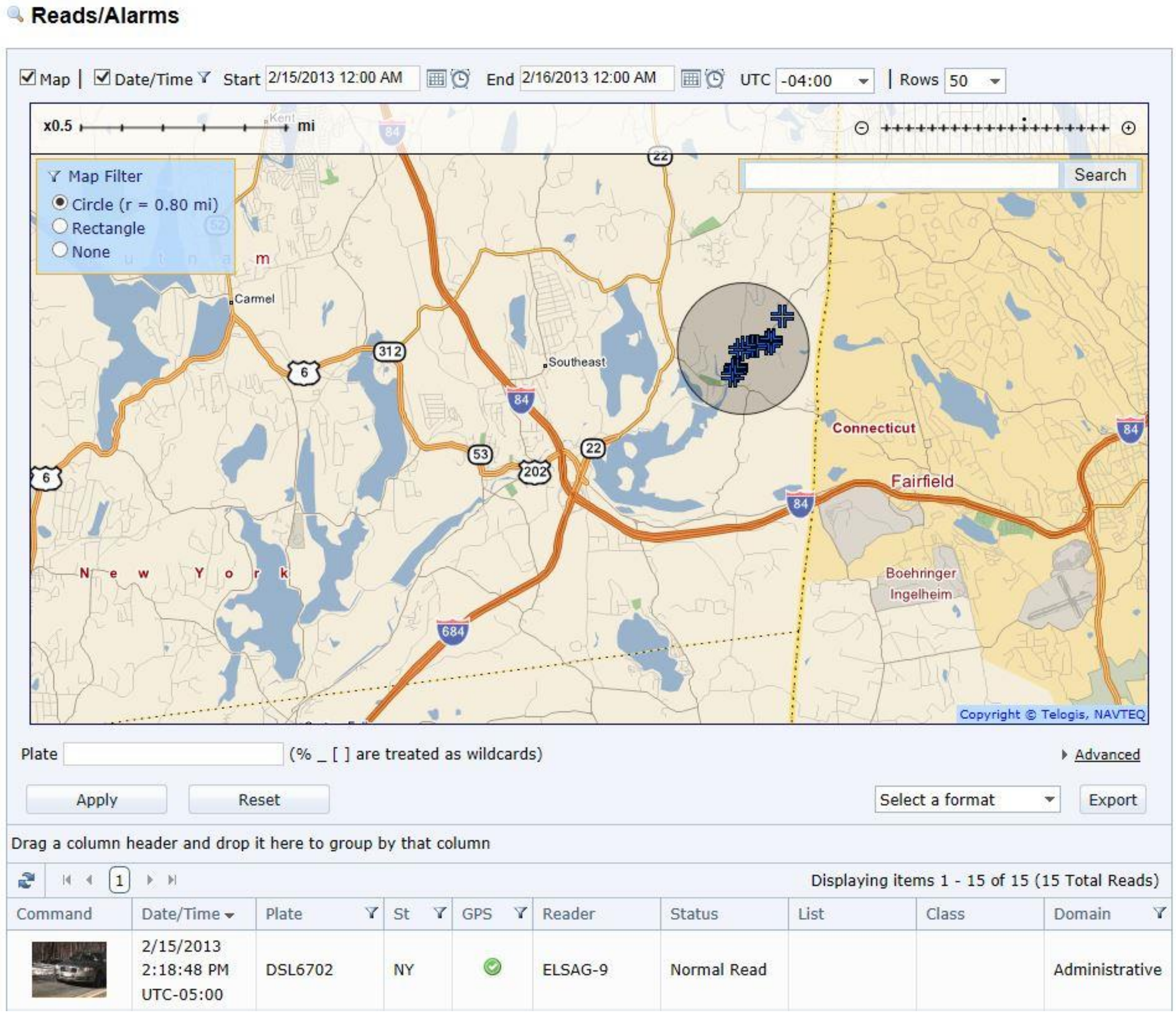
Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	2/15/2013 2:18:48 PM UTC-05:00	DSL6702	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 54 — Map Filter Selected

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Referring to Figure 55, once you have selected the area of the map to be filtered press the **Apply** button. The listing of plate reads below the map diminishes to include only the ones visible on the displayed part of the map.

> **NOTE:** The list has now diminished to the supporting details for only the reads shown on that map segment. In this example, the reads have been reduced from 320 to 15 reads.



Reads/Alarms

☑ Map | ☑ Date/Time Start 2/15/2013 12:00 AM End 2/16/2013 12:00 AM UTC -04:00 | Rows 50

Map Filter
● Circle (r = 0.80 mi)
○ Rectangle
○ None

Plate (% _ [ ] are treated as wildcards)

Drag a column header and drop it here to group by that column

Displaying items 1 - 15 of 15 (15 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	2/15/2013 2:18:48 PM UTC-05:00	DSL6702	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 55 — Map Filter Applied Results

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Convoy Search

The Convoy Search feature allows you to identify plates that are seen together frequently.

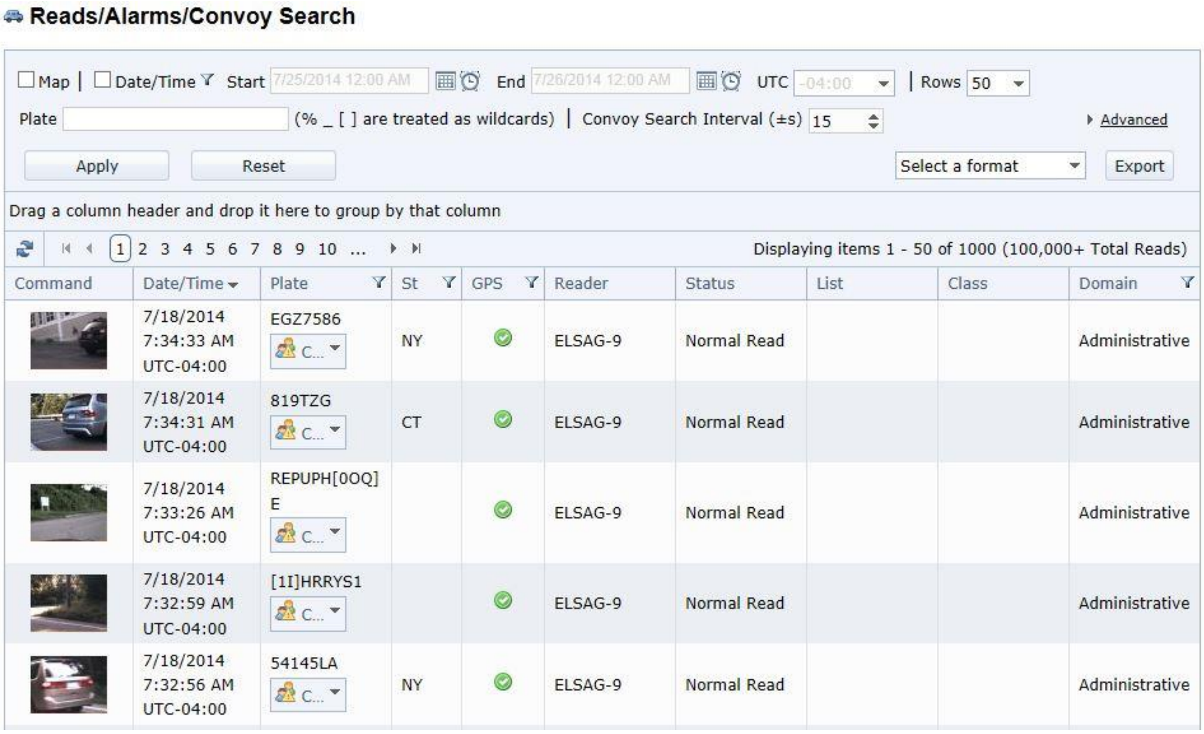
> **NOTE:** Currently, Convoy Search is not configured to work with remote servers. If a result is returned from a remote server, no Convoy icon will be displayed.

Examples of a **Convoy Search** are as follows:

- Smugglers have spread their cargo throughout multiple vehicles in a traveling caravan to lower the risk of losing their supply in its entirety. If one of the vehicle(s) is stopped along the way, the others would still be able to pass through undetected. Convoy Search can be used to detect one such caravan of vehicles.
- An officer is concerned about vehicles that may be following them. By using Convoy search, it can be seen if a vehicle has been traveling in the same locations that they have been.

To perform a convoy search perform the following steps:

(1) Select **Data Mining > Convoy Search**.



Reads/Alarms/Convoy Search

☐ Map | ☐ Date/Time Start 7/25/2014 12:00 AM End 7/26/2014 12:00 AM UTC -04:00 | Rows 50

Plate (% _ [ ] are treated as wildcards) | Convoy Search Interval (±s) 15

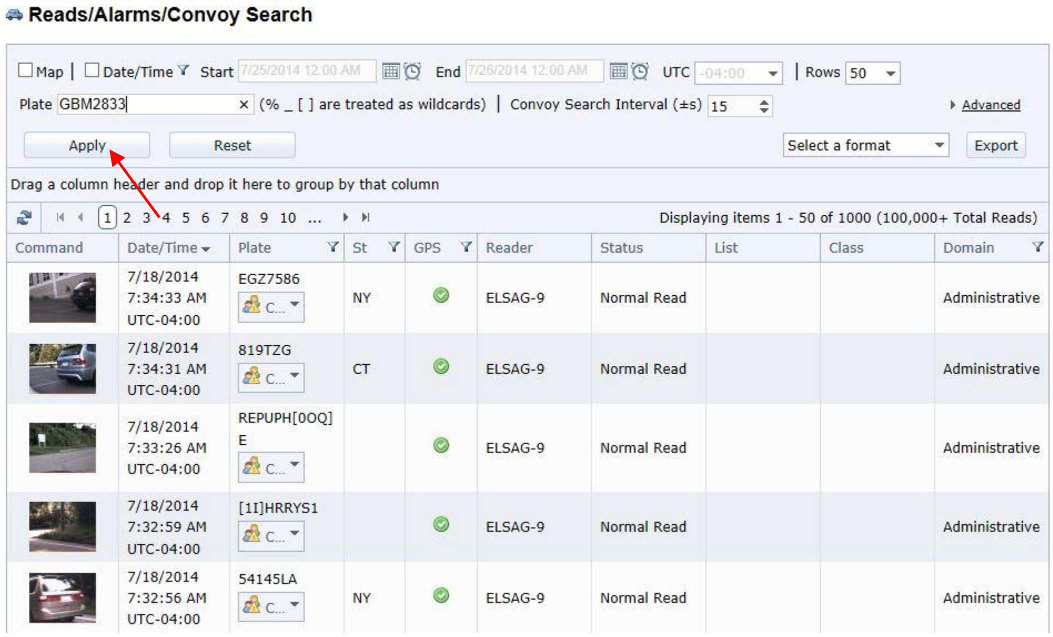
Displaying items 1 - 50 of 1000 (100,000+ Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	7/18/2014 7:34:33 AM UTC-04:00	EGZ7586 C...	NY	✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:34:31 AM UTC-04:00	819TZG C...	CT	✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:33:26 AM UTC-04:00	REPUPH[0OQ]E C...		✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:32:59 AM UTC-04:00	[1I]HRRYS1 C...		✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:32:56 AM UTC-04:00	54145LA C...	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 56 — Convoy Search Initial Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(2) Perform a normal search for the primary plate you are interested in, using the standard search parameters and click **Apply**.



Reads/Alarms/Convoy Search

□ Map | □ Date/Time Start 7/25/2014 12:00 AM End 7/26/2014 12:00 AM UTC -04:00 | Rows 50

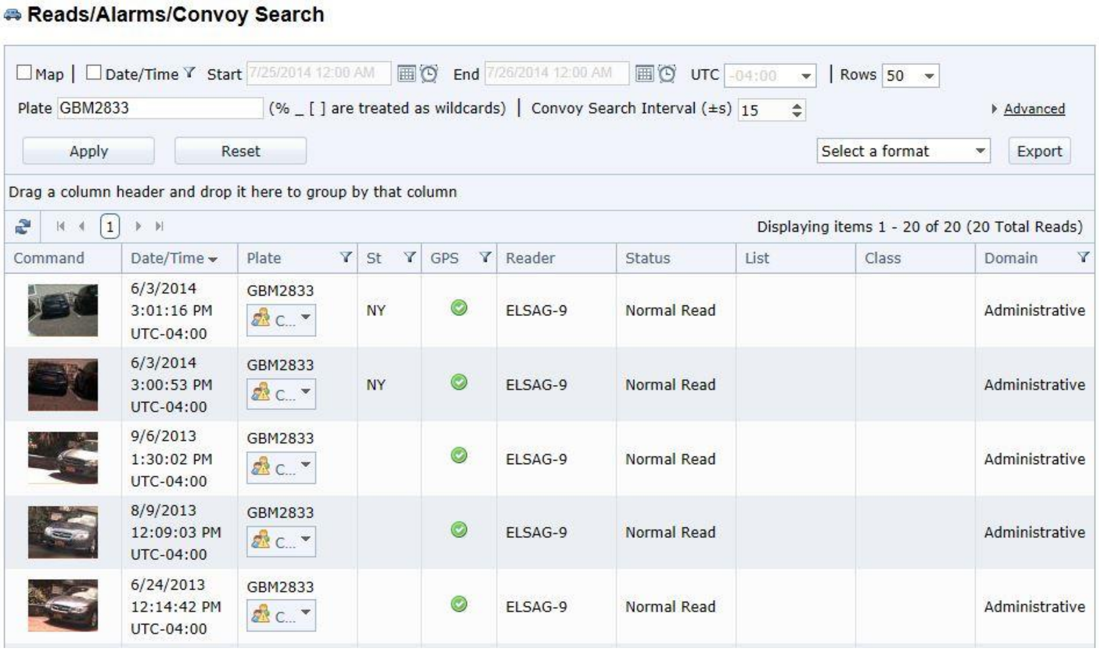
Plate GBM2833 (% _ [ ] are treated as wildcards) | Convoy Search Interval (±s) 15

Displaying items 1 - 50 of 1000 (100,000+ Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	7/18/2014 7:34:33 AM UTC-04:00	EGZ7586	NY	✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:34:31 AM UTC-04:00	819TZG	CT	✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:33:26 AM UTC-04:00	REPUPH[0OQ]E		✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:32:59 AM UTC-04:00	[1I]HRRYS1		✓	ELSAG-9	Normal Read			Administrative
	7/18/2014 7:32:56 AM UTC-04:00	54145LA	NY	✓	ELSAG-9	Normal Read			Administrative

Figure 57 — Convoy Search Parameters

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.



Reads/Alarms/Convoy Search

□ Map | □ Date/Time Start 7/25/2014 12:00 AM End 7/26/2014 12:00 AM UTC -04:00 | Rows 50

Plate GBM2833 (% _ [ ] are treated as wildcards) | Convoy Search Interval (±s) 15

Drag a column header and drop it here to group by that column

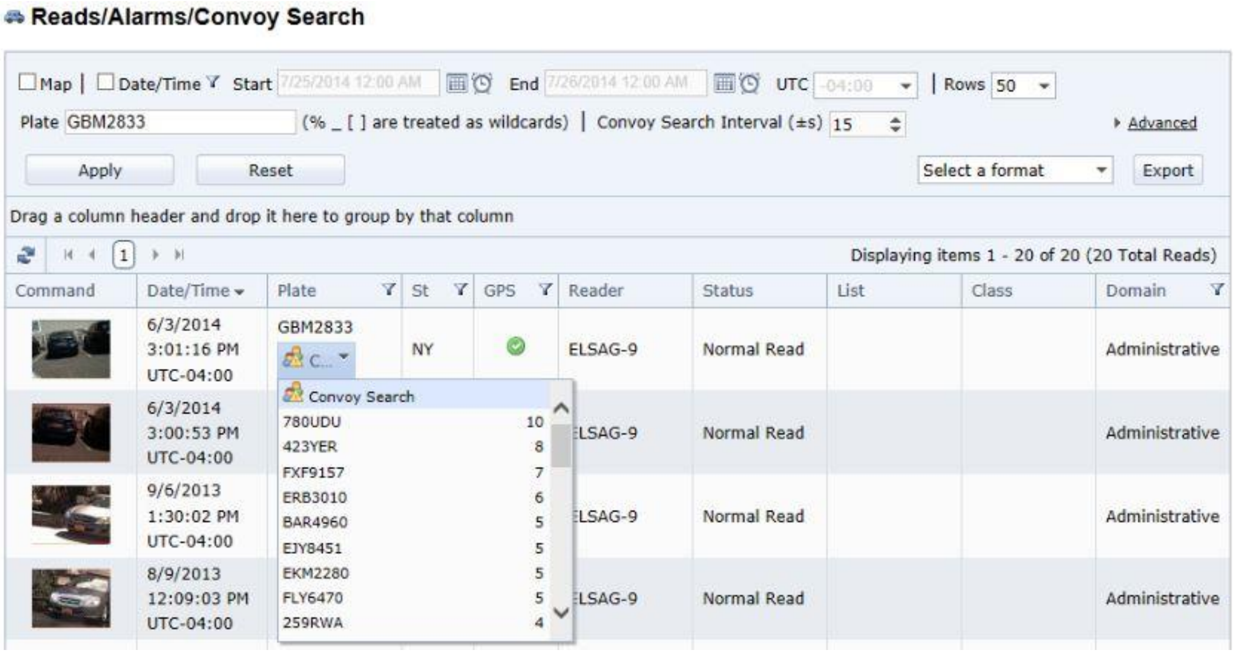
Displaying items 1 - 20 of 20 (20 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	6/3/2014 3:01:16 PM UTC-04:00	GBM2833 C...	NY	✓	ELSAG-9	Normal Read			Administrative
	6/3/2014 3:00:53 PM UTC-04:00	GBM2833 C...	NY	✓	ELSAG-9	Normal Read			Administrative
	9/6/2013 1:30:02 PM UTC-04:00	GBM2833 C...		✓	ELSAG-9	Normal Read			Administrative
	8/9/2013 12:09:03 PM UTC-04:00	GBM2833 C...		✓	ELSAG-9	Normal Read			Administrative
	6/24/2013 12:14:42 PM UTC-04:00	GBM2833 C...		✓	ELSAG-9	Normal Read			Administrative

Figure 58 — Convoy Search Initial Results

(3) Press the **Convoy** icon found under the plate field.

(4) You will see a list of all the plate reads that are within the specified interval along with a number that reports how often the second plate was seen with the first.



Reads/Alarms/Convoy Search

□ Map | □ Date/Time Start 7/25/2014 12:00 AM End 7/26/2014 12:00 AM UTC -04:00 | Rows 50

Plate GBM2833 (% _ [ ] are treated as wildcards) | Convoy Search Interval (±s) 15

Drag a column header and drop it here to group by that column

Displaying items 1 - 20 of 20 (20 Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	6/3/2014 3:01:16 PM UTC-04:00	GBM2833 C...	NY	✓	ELSAG-9	Normal Read			Administrative
	6/3/2014 3:00:53 PM UTC-04:00				ELSAG-9	Normal Read			Administrative
	9/6/2013 1:30:02 PM UTC-04:00				ELSAG-9	Normal Read			Administrative
	8/9/2013 12:09:03 PM UTC-04:00				ELSAG-9	Normal Read			Administrative

Convoy Search

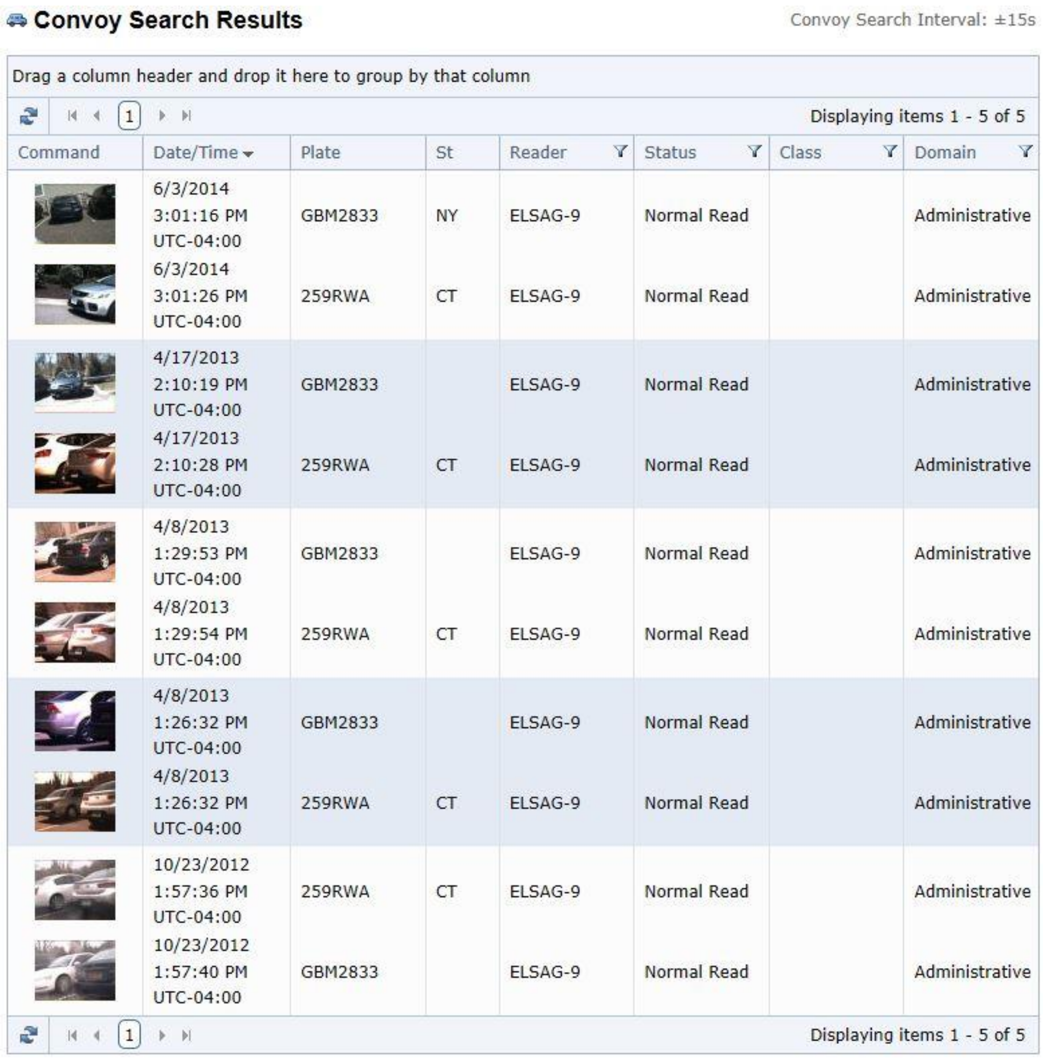
780UDU	10
423YER	8
FXF9157	7
ERB3010	6
BAR4960	5
EJY8451	5
EKM2280	5
FLY6470	5
259RWA	4

Figure 59 — Convoy Results List

The interval is configurable from a minimum of one second to a maximum of 86,400 seconds (24 hours). The default interval is 15 seconds before and after the primary read. You can manually change the interval by changing the value in the Convoy Search Interval numeric text box. Remember to click Apply when finished so your changes can take effect.

(5) Select a plate number from the results list to pop up a new window with the pairs of reads and their associated images. Click in either image to see the details of both reads.

NOTE: Each window displays two records, the primary and the secondary, in order of the time they were recorded.



Convoy Search Results

Convoy Search Interval: ±15s

Drag a column header and drop it here to group by that column

Displaying items 1 - 5 of 5

Command	Date/Time	Plate	St	Reader	Status	Class	Domain
	6/3/2014 3:01:16 PM UTC-04:00	GBM2833	NY	ELSAG-9	Normal Read		Administrative
	6/3/2014 3:01:26 PM UTC-04:00	259RWA	CT	ELSAG-9	Normal Read		Administrative
	4/17/2013 2:10:19 PM UTC-04:00	GBM2833		ELSAG-9	Normal Read		Administrative
	4/17/2013 2:10:28 PM UTC-04:00	259RWA	CT	ELSAG-9	Normal Read		Administrative
	4/8/2013 1:29:53 PM UTC-04:00	GBM2833		ELSAG-9	Normal Read		Administrative
	4/8/2013 1:29:54 PM UTC-04:00	259RWA	CT	ELSAG-9	Normal Read		Administrative
	4/8/2013 1:26:32 PM UTC-04:00	GBM2833		ELSAG-9	Normal Read		Administrative
	4/8/2013 1:26:32 PM UTC-04:00	259RWA	CT	ELSAG-9	Normal Read		Administrative
	10/23/2012 1:57:36 PM UTC-04:00	259RWA	CT	ELSAG-9	Normal Read		Administrative
	10/23/2012 1:57:40 PM UTC-04:00	GBM2833		ELSAG-9	Normal Read		Administrative

Displaying items 1 - 5 of 5

Figure 60 — Convoy Pairs Sample Display

When you have finished a convoy search, you can reproduce the same results at any time. Save the final results page URL as a Favorite or Bookmark so that you can run the same report by clicking on the Favorite.

Chapter 5 — User Configuration

Assigning Privileges

Privileges are assigned to users by means of groups. When you create a group, you assign it a set of privileges for some or all EOC features as well as access to some or all sets of data (domains) within the EOC database.

A group can have the following privileges granted or denied based on EOC features:

- Data Mining
- Lists
- Monitoring Tools
- System and
- User Config

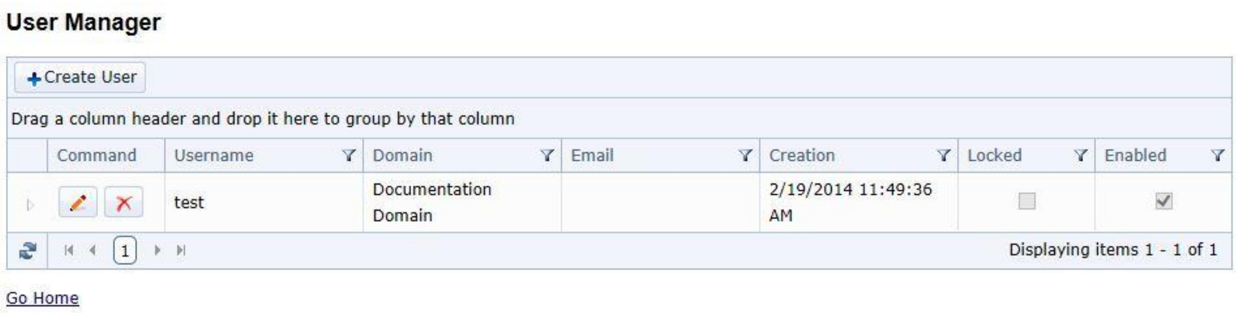
A group can have the following privileges granted or denied on a particular domain’s data:

- View Lists
- Modify Lists
- Access Plate Read data for:
  - Alarm Validation
  - Modify
  - Basic Search
  - Convoy Search
  - Cross Search, and
  - Statistics.
- System Configuration
  - View, and
  - Modify.
- View User Groups
- Modify User Groups
- View Users, and
- Modify Users.

Managing Users — SQL Server Mode

To create a User perform the following steps:

(1) Select **User Config > User Manager** from the menu bar across the top of the main screen.


User Manager
+Create User
Drag a column header and drop it here to group by that column
Displaying items 1 - 1 of 1
Go Home

	Command	Username	Domain	Email	Creation	Locked	Enabled
▷	✎ ✕	test	Documentation Domain		2/19/2014 11:49:36 AM	□	☑

Figure 61 — User Manager Screen

(2) Press the "+ Create User" button and the screen shown in Figure 62 will appear.

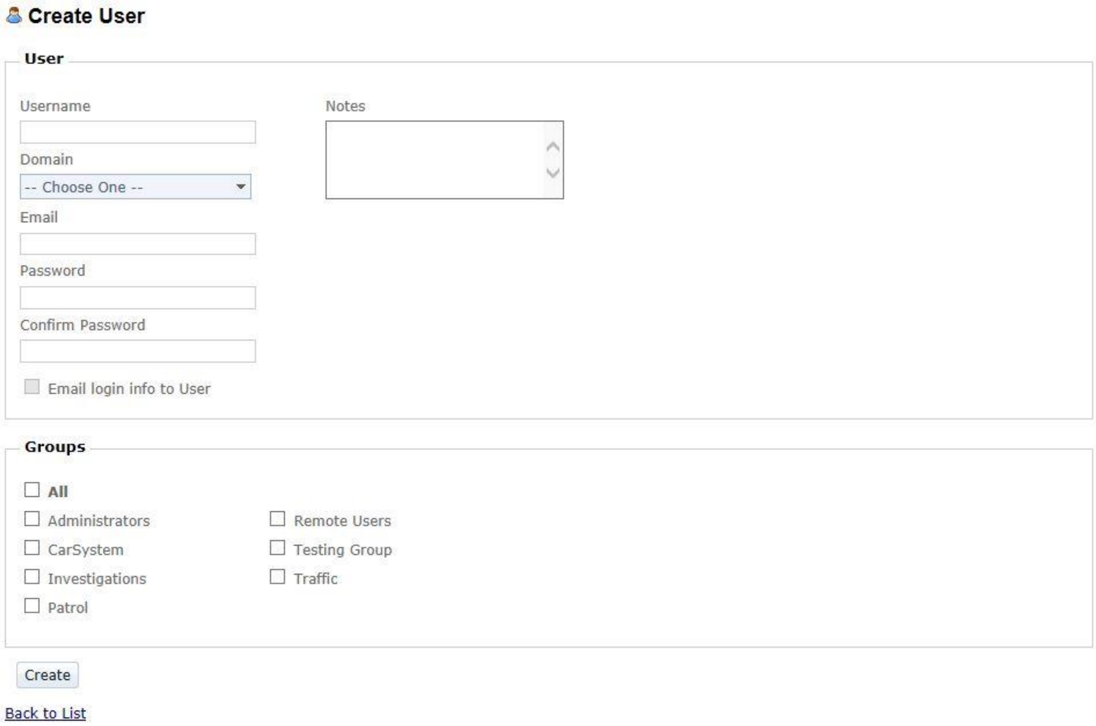


Figure 62 — SQL Server Mode Create User Initial Screen

(3) Type in the **Username** for the new user.

(4) Select the EOC **Domain** in which you want to create this user. You will only see domains to which you have access.

(5) Enter the **Email Address** associated with the user.

(6) Add a **Password** and then confirm the password by typing it in again.

(7) The optional **Notes** box can be used to spell out a user’s name or provide any notes needed.

(8) Select the checkbox to email the login information to the new user. (The message will also contain the URL to the EOC implementation.)

(9) Select the groups to which the new user will belong by checking the boxes.

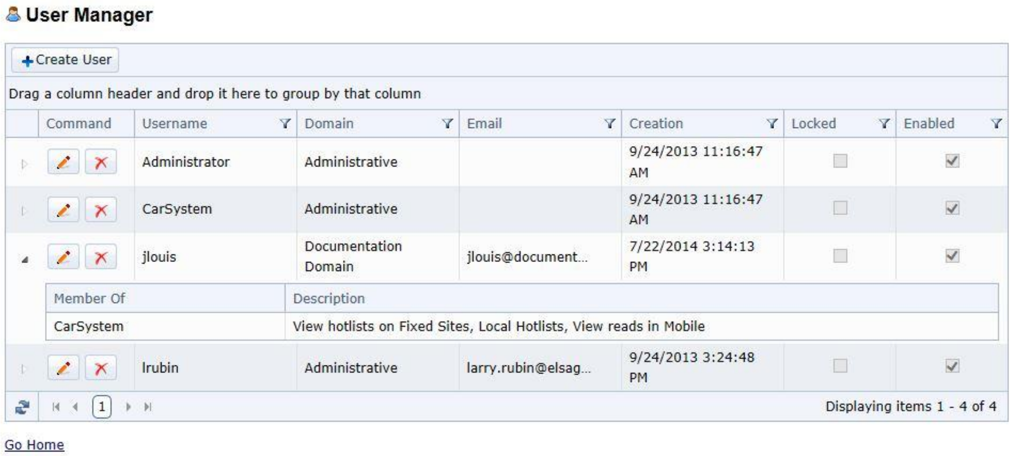
(10)Press **Create** to create the new user.

View a User’s Details

You can view a user account’s details, including the following attributes:

- Username
- Domain
- Email Address
- Creation date and time, and
- Whether the user is Enabled or Locked.

To view a user’s details, select **User Config > User Manager** from the menu bar across the top of the main screen and the screen shown below in Figure 63 will appear. This allows you to view a list of all users. Clicking on the triangle will display to what Groups a user is assigned.



User Manager
+Create User
Drag a column header and drop it here to group by that column

	Command	Username	Domain	Email	Creation	Locked	Enabled
▷	✎ ✗	Administrator	Administrative		9/24/2013 11:16:47 AM	□	☑
▷	✎ ✗	CarSystem	Administrative		9/24/2013 11:16:47 AM	□	☑
◢	✎ ✗	jlouis	Documentation Domain	jlouis@document...	7/22/2014 3:14:13 PM	□	☑
▷	✎ ✗	lrubin	Administrative	larry.rubin@elsag...	9/24/2013 3:24:48 PM	□	☑

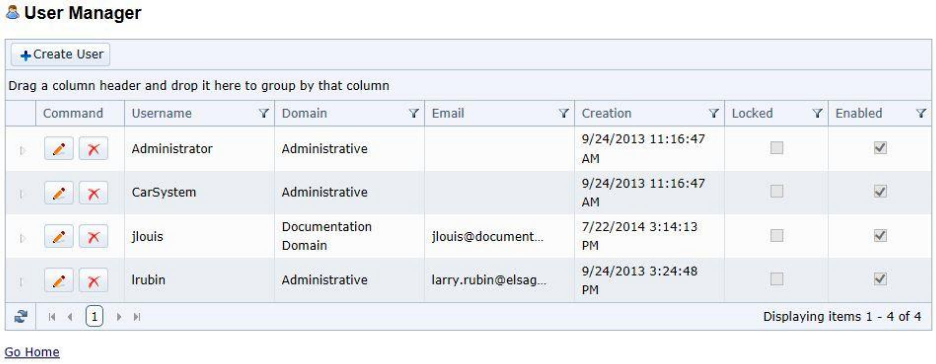
Member Of	Description
CarSystem	View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile

Figure 63 — SQL Server Mode User Details Screen

Edit a User’s Details, including Password

To edit a user’s details, perform the following steps:

(1) Select **User Config > User Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 64.



User Manager

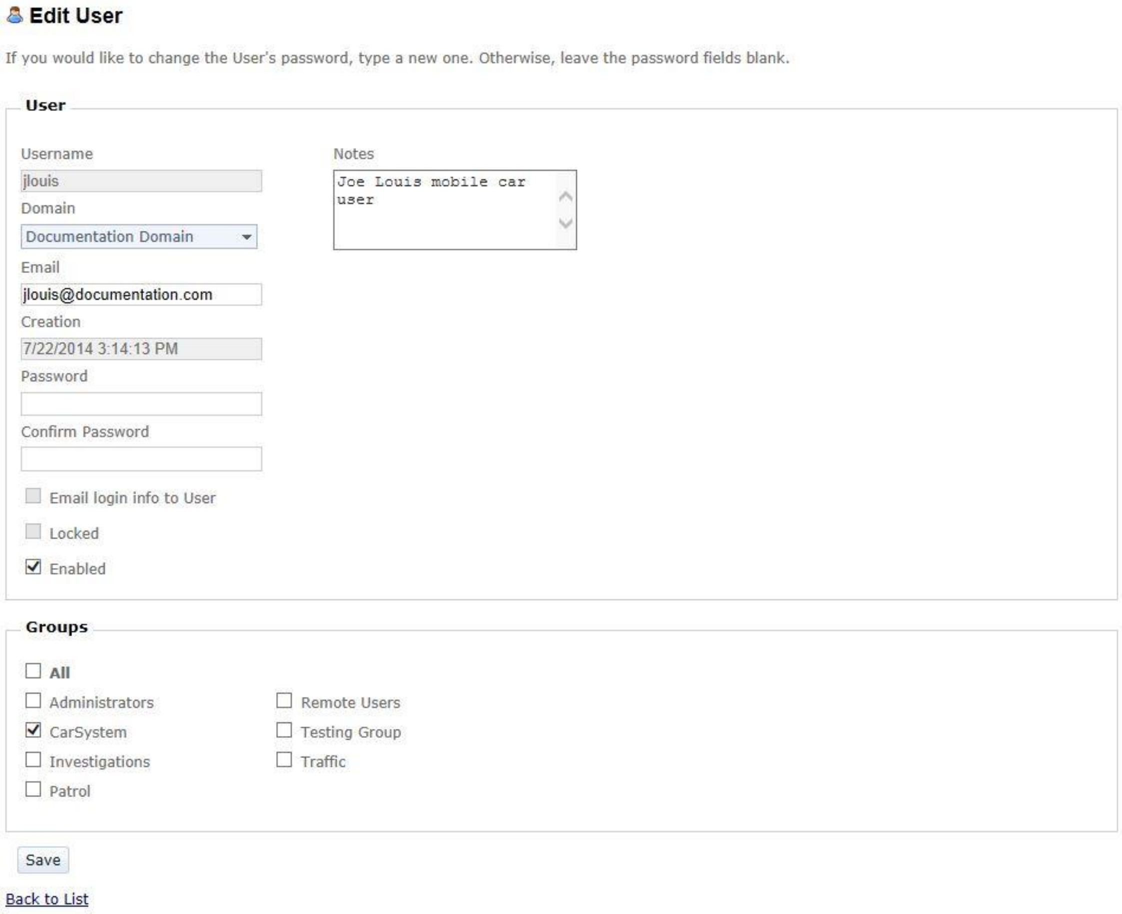
+Create User
Drag a column header and drop it here to group by that column

	Command	Username	Domain	Email	Creation	Locked	Enabled
▷	✎ ✕	Administrator	Administrative		9/24/2013 11:16:47 AM	□	☑
▷	✎ ✕	CarSystem	Administrative		9/24/2013 11:16:47 AM	□	☑
▷	✎ ✕	jlouis	Documentation Domain	jlouis@document...	7/22/2014 3:14:13 PM	□	☑
▷	✎ ✕	lrubin	Administrative	larry.rubin@elsag...	9/24/2013 3:24:48 PM	□	☑

1
Displaying items 1 - 4 of 4
Go Home

Figure 64 — SQL Server Mode User Details Screen

(2) Press the **Edit** Icon (pencil) next to the user whose attributes you want to edit and a screen similar to the one shown in Figure 65 will appear.



Edit User

If you would like to change the User's password, type a new one. Otherwise, leave the password fields blank.

User

Username: jlouis

Domain: Documentation Domain

Email: jlouis@documentation.com

Creation: 7/22/2014 3:14:13 PM

Password:

Confirm Password:

Notes: Joe Louis mobile car user

□ Email login info to User

□ Locked

☑ Enabled

Groups

□ All

□ Administrators

☑ CarSystem

□ Investigations

□ Patrol

□ Remote Users

□ Testing Group

□ Traffic

Figure 65 — SQL Server Mode Edit User Screen

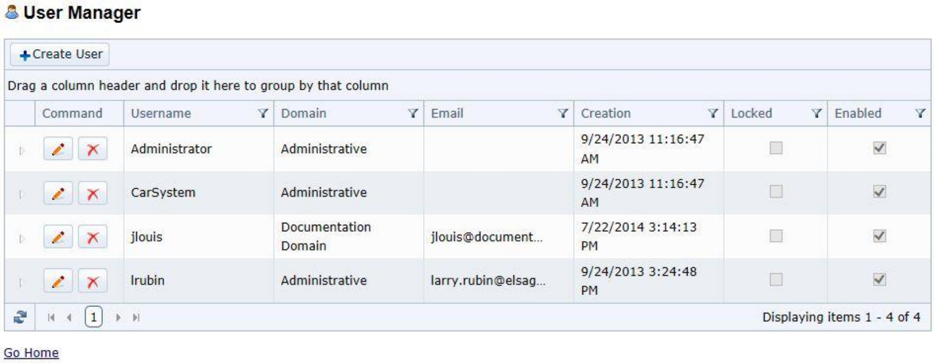
(3) Edit the fields you need to edit.

(4) Press the **Save** button to save the changes.

Delete a User

To delete a user, perform the following steps:

(1) Select **User Config > User Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 66.



User Manager

+Create User

Drag a column header and drop it here to group by that column

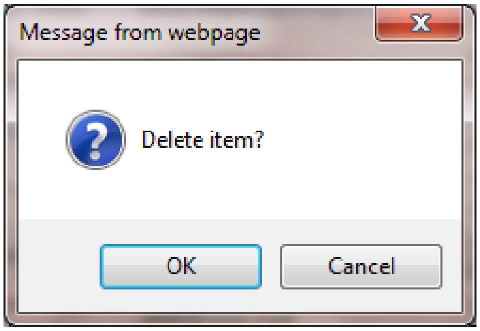
Command	Username	Domain	Email	Creation	Locked	Enabled
✎ ✗	Administrator	Administrative		9/24/2013 11:16:47 AM	□	☑
✎ ✗	CarSystem	Administrative		9/24/2013 11:16:47 AM	□	☑
✎ ✗	jlouis	Documentation Domain	jlouis@document...	7/22/2014 3:14:13 PM	□	☑
✎ ✗	lrubin	Administrative	larry.rubin@elsag...	9/24/2013 3:24:48 PM	□	☑

Displaying items 1 - 4 of 4

Go Home

Figure 66 — SQL Server Mode User Details Screen

(2) Press the **Delete Icon** (red X) next to the user you want to delete and you will see the screen shown in Figure 67.



Message from webpage

Delete item?

Figure 67 — SQL Server Mode Delete User Confirmation

(3) Press **OK**. The user account is deleted.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Managing Users — Active Directory Mode

Managing users in Active Directory Mode is slightly different from managing them in SQL Server Mode because authentication in Active Directory Mode is handled by Windows Active Directory.

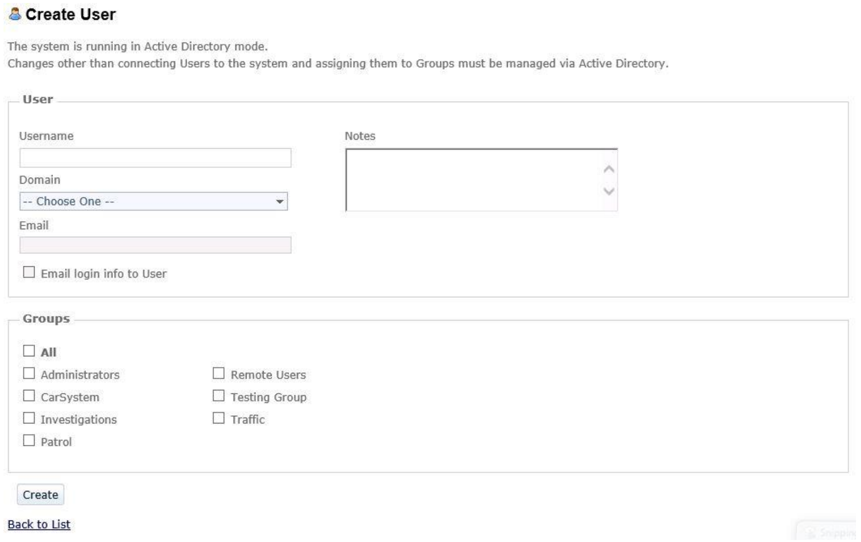
> **NOTE:** When you create a user in EOC, you are associating an existing Windows username and password with an EOC user account. Therefore, when you manage users in EOC in Active Directory Mode, any changes you make to an EOC user **will not be reflected** in the Windows user account. Likewise if you delete a user, the user will only be deleted inside the EOC, not in Windows.

Create a User

> **NOTE:** If a user does not already exist in Windows Active Directory, you will not be able to create an EOC user; create the Windows Active Directory user account first.

(1) Select **User Config > User Manager** from the menu. You will see a display of all the EOC current users. Note that the display will remind you that you are running in Active Directory Mode.

(2) Press the "+ Create User" button and the screen shown in Figure 68 will appear.



Create User

The system is running in Active Directory mode.
Changes other than connecting Users to the system and assigning them to Groups must be managed via Active Directory.

User

Username

Notes

Domain

-- Choose One --

Email

□ Email login info to User

Groups

□ All

□ Administrators □ Remote Users

□ CarSystem □ Testing Group

□ Investigations □ Traffic

□ Patrol

Create

Back to List

Figure 68 — Active Directory Mode Create User Initial Screen

(3) Type in a **Username** for the new user. The username must be in the same format as the Windows Active Directory username, for example, **<u>joe.louis</u>**. As you type characters in, the EOC system will display possibilities that you can select.

NOTE: There is no place to set a password, since Active Directory Mode uses Windows authentication to control access to EOC. The EOC user's password will be the same as the password to the Window user account. The **Email Address** will automatically fill in once you enter the existing Windows user.

(4) Select the EOC **Domain** in which you want to create this user. You will only see domains to which you have access.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(5) Select the checkbox to email the login information to the new user. (The message will also contain the URL to the EOC implementation.)

(6) The optional **Notes** box can be used to spell out a user's name or provide any notes needed.

(7) Select the groups to which the new user will belong by checking the boxes.

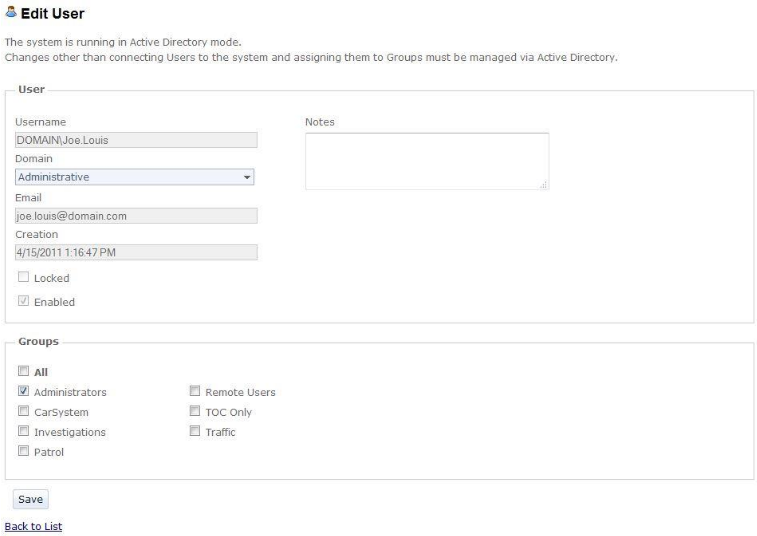
(8) Press **Create** to create the new user.

View or Edit a User's Details

You use the same procedure to view a user's details or to edit a user's details. Use the steps that follow:

(1) Select **User Config > User Manager** from the menu. You will see a display of all the EOC current users. Note that the display will remind you that you are running in Active Directory Mode.

(2) Press the **Edit** button next to the user whose attributes you want to view or edit and a screen similar to the one shown in Figure 69 will appear.



Edit User

The system is running in Active Directory mode.
Changes other than connecting Users to the system and assigning them to Groups must be managed via Active Directory.

User

Username: DOMAIN\Joe.Louis

Domain: Administrative

Email: joe.louis@domain.com

Creation: 4/15/2011 1:16:47 PM

Notes:

☐ Locked

☑ Enabled

Groups

☐ All

☑ Administrators

☐ CarSystem

☐ Investigations

☐ Patrol

☐ Remote Users

☐ TOC Only

☐ Traffic

Figure 69 — Active Directory Mode View/Edit User Screen

(3) Non-editable fields will be grayed out. Edit fields that you want to change.

(4) Press the **Save** button to save the changes.

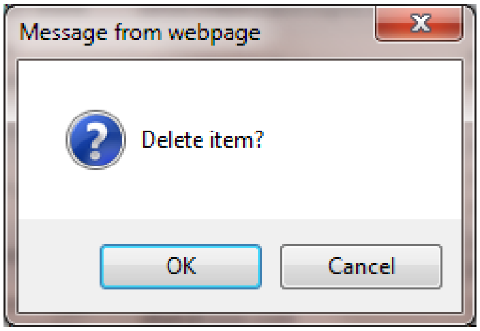
Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Delete a User

To delete a user perform the following steps:

(1) Select **User Config > User Manager** from the menu. You will see a display of all the EOC current users. Note that the display will remind you that you are running in Active Directory Mode.

(2) Press the **Delete Icon** (red X) next to the user whose attributes you want to view or edit. You will see the screen shown in Figure 70.


Message from webpage

Delete item?

Figure 70 — Active Directory Mode Delete User Confirmation

(3) Press **OK**. The EOC user account is deleted. The windows active directory user account is unaffected.

Managing Groups

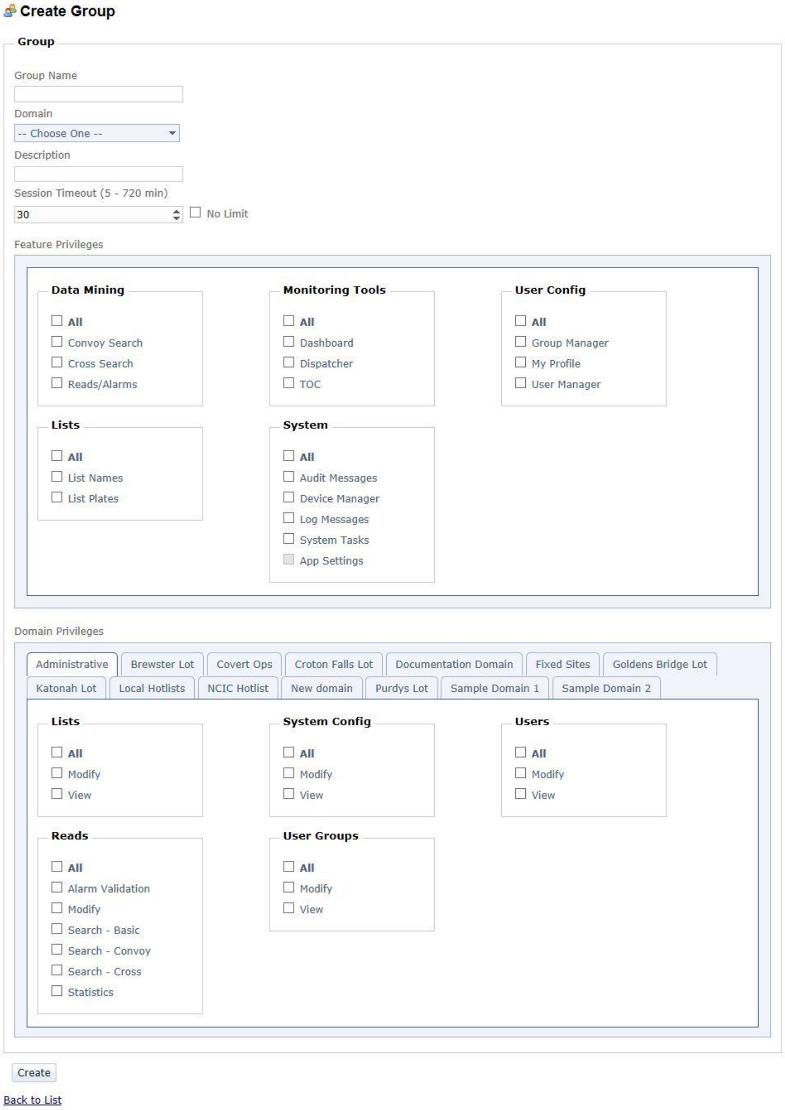
Creating and managing groups operates exactly the same in SQL Server Mode and Active Directory Mode.

Create a Group Procedure

To create a group, perform the following steps:

(1) Select **User Config > Group Manager** from the menu bar across the top of the main screen.

(2) Press the “+ Create Group” button and the screen shown in Figure 71 will appear.



Create Group

Group

Group Name

Domain
-- Choose One --

Description

Session Timeout (5 - 720 min)
30 □ No Limit

Feature Privileges

Data Mining
□ **All**
□ Convoy Search
□ Cross Search
□ Reads/Alarms

Monitoring Tools
□ **All**
□ Dashboard
□ Dispatcher
□ TOC

User Config
□ **All**
□ Group Manager
□ My Profile
□ User Manager

Lists
□ **All**
□ List Names
□ List Plates

System
□ **All**
□ Audit Messages
□ Device Manager
□ Log Messages
□ System Tasks
□ App Settings

Domain Privileges

Lists
□ **All**
□ Modify
□ View

System Config
□ **All**
□ Modify
□ View

Users
□ **All**
□ Modify
□ View

Reads
□ **All**
□ Alarm Validation
□ Modify
□ Search - Basic
□ Search - Convoy
□ Search - Cross
□ Statistics

User Groups
□ **All**
□ Modify
□ View

Figure 71 — Create Group Initial Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(3) Type in the Group Name for the new group.

(4) Select the EOC **Domain** in which you want to create this group from the **Domain** dropdown. You will only see domains to which you have access. (The named domain tabs across the bottom allow you to specify the permissions that members of this group will have in each of those domains.)

(5) Enter a **Description** for the group.

(6) Add a **Session Timeout** in minutes. This controls how long a session initiated by someone in this group will stay active if there is no activity.

(7) Select the checkboxes to assign EOC Feature Privileges for this group.

(8) Select the checkboxes to assign individual Domain Privileges for this group.

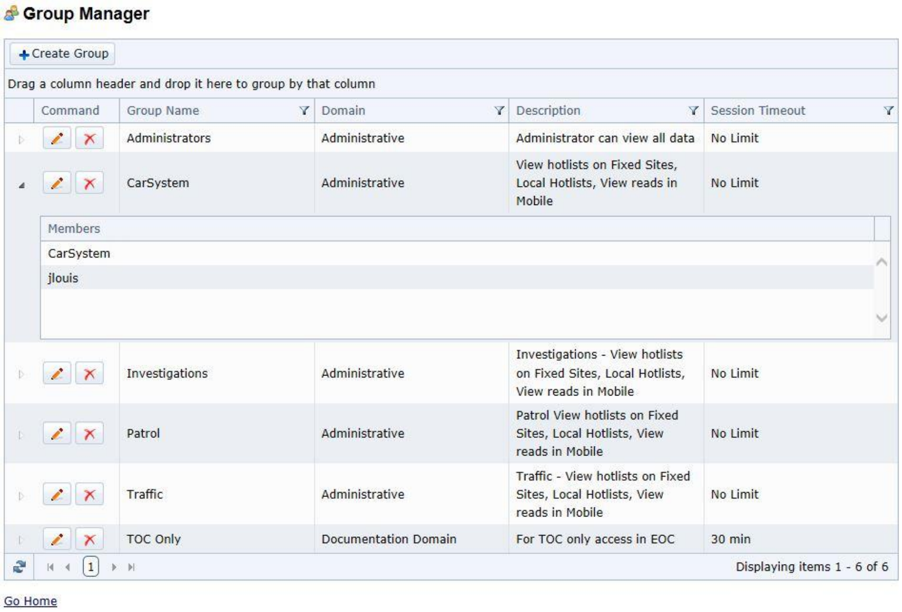
(9) Press **Create** to create the new group.

View a Group's Details

You can view a group's details, including the following attributes:

- Group Name
- Domain — Domain the group belongs to
- Description — Group's description, and
- Session Timeout — How long a session will stay active if there is no activity.

To see a group's details, select **User Config > Group Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 72. This allows you to view a list of all groups. Clicking on the triangle will display all Users assigned to the Group.


Group Manager
+Create Group
Drag a column header and drop it here to group by that column

Command	Group Name	Domain	Description	Session Timeout
	Administrators	Administrative	Administrator can view all data	No Limit
	CarSystem	Administrative	View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit

Members
CarSystem
jlouis

Command	Group Name	Domain	Description	Session Timeout
	Investigations	Administrative	Investigations - View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
	Patrol	Administrative	Patrol View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
	Traffic	Administrative	Traffic - View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
	TOC Only	Documentation Domain	For TOC only access in EOC	30 min

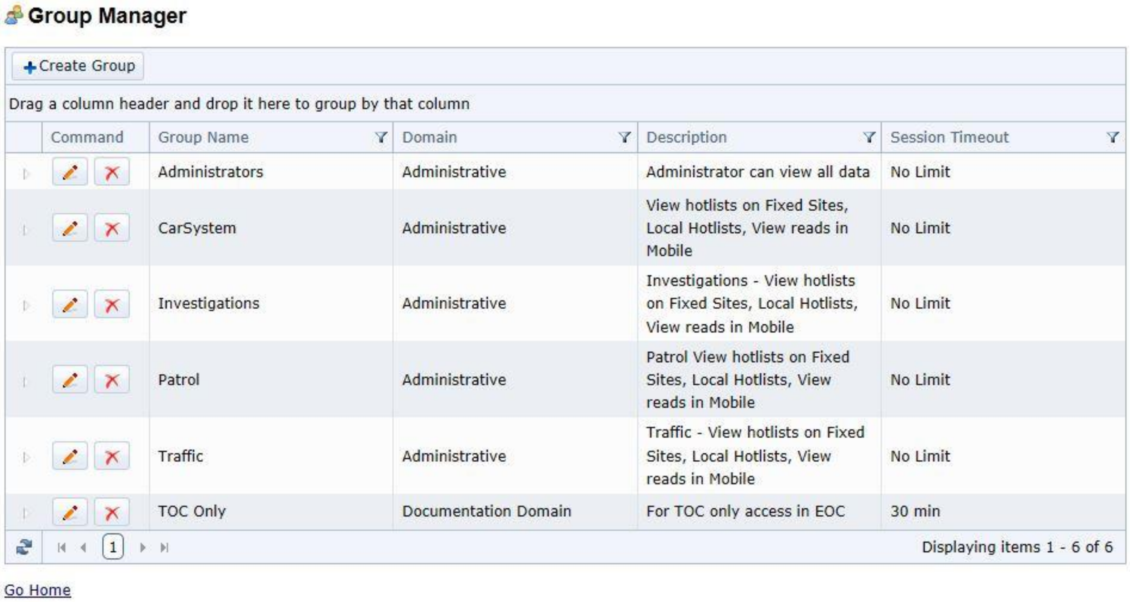
Figure 72 — Group Details Screen Showing Members

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Edit a Group

To edit a group perform the following steps:

(1) Select **User Config > Group Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 73. Press the **Edit Icon** (pencil) next to the group whose attributes you want to edit.



Drag a column header and drop it here to group by that column

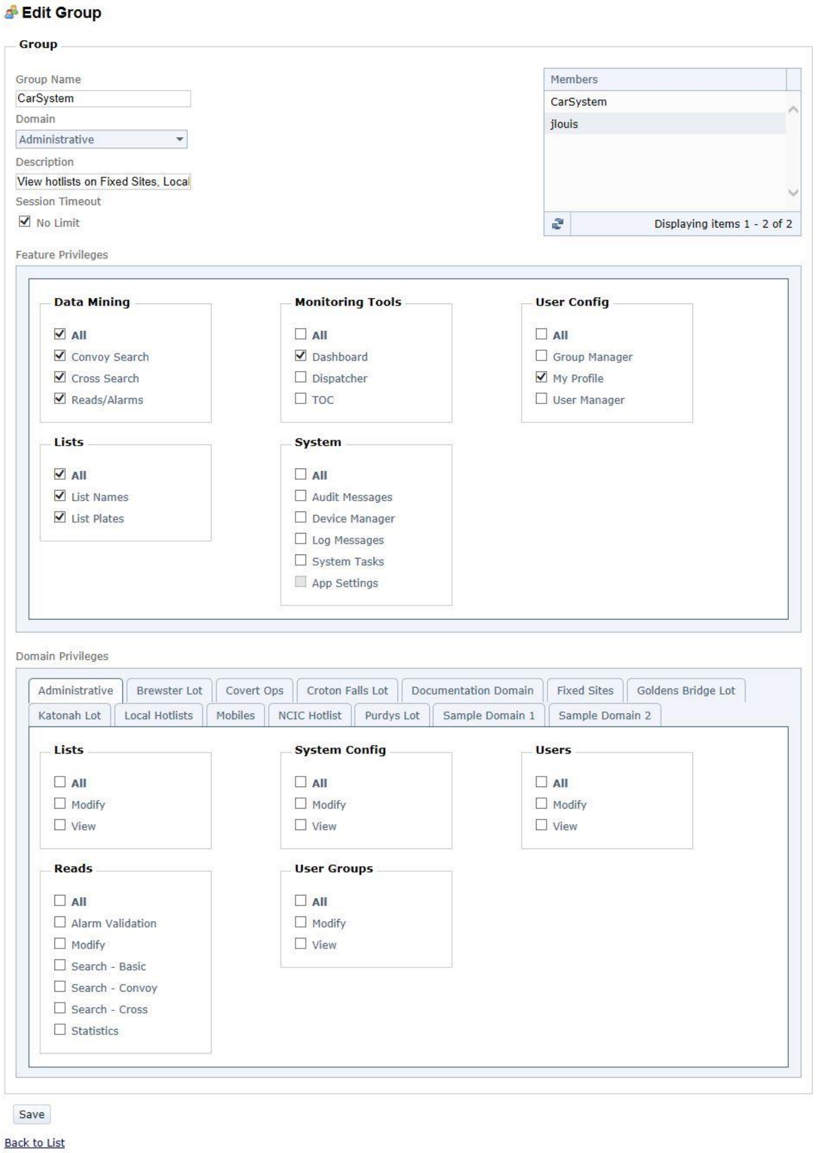
	Command	Group Name	Domain	Description	Session Timeout
▷	✎ ✗	Administrators	Administrative	Administrator can view all data	No Limit
▷	✎ ✗	CarSystem	Administrative	View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
▷	✎ ✗	Investigations	Administrative	Investigations - View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
▷	✎ ✗	Patrol	Administrative	Patrol View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
▷	✎ ✗	Traffic	Administrative	Traffic - View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
▷	✎ ✗	TOC Only	Documentation Domain	For TOC only access in EOC	30 min

Displaying items 1 - 6 of 6

Figure 73 — Group Details Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(2) Referring to Figure 74, shows the **Edit Group** screen.



Edit Group

Group

Group Name: CarSystem

Domain: Administrative

Description: View hotlists on Fixed Sites, Local

Session Timeout: ☑ No Limit

Members:
- CarSystem
- jlouis

Displaying items 1 - 2 of 2

Feature Privileges

Data Mining
- ☑ All
- ☑ Convoy Search
- ☑ Cross Search
- ☑ Reads/Alarms

Monitoring Tools
- ☐ All
- ☑ Dashboard
- ☐ Dispatcher
- ☐ TOC

User Config
- ☐ All
- ☐ Group Manager
- ☑ My Profile
- ☐ User Manager

Lists
- ☑ All
- ☑ List Names
- ☑ List Plates

System
- ☐ All
- ☐ Audit Messages
- ☐ Device Manager
- ☐ Log Messages
- ☐ System Tasks
- ☐ App Settings

Domain Privileges

Lists
- ☐ All
- ☐ Modify
- ☐ View

System Config
- ☐ All
- ☐ Modify
- ☐ View

Users
- ☐ All
- ☐ Modify
- ☐ View

Reads
- ☐ All
- ☐ Alarm Validation
- ☐ Modify
- ☐ Search - Basic
- ☐ Search - Convoy
- ☐ Search - Cross
- ☐ Statistics

User Groups
- ☐ All
- ☐ Modify
- ☐ View

Figure 74 — Edit Group Screen

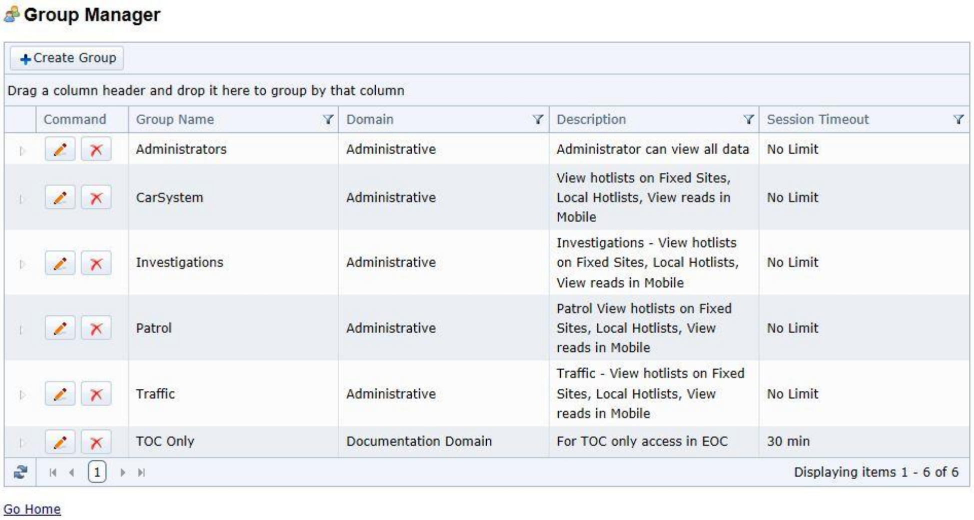
(3) Edit the fields and/or privileges you need to edit.

(4) Press the **Save** button to save the changes.

Delete a Group

To delete a group perform the following steps:

(1) Select **User Config > Group Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 75.



Group Manager

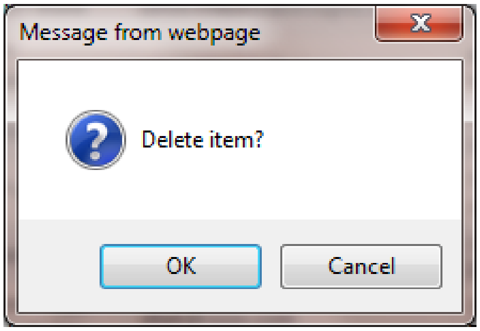
Drag a column header and drop it here to group by that column

Command	Group Name	Domain	Description	Session Timeout
✎ ✕	Administrators	Administrative	Administrator can view all data	No Limit
✎ ✕	CarSystem	Administrative	View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
✎ ✕	Investigations	Administrative	Investigations - View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
✎ ✕	Patrol	Administrative	Patrol View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
✎ ✕	Traffic	Administrative	Traffic - View hotlists on Fixed Sites, Local Hotlists, View reads in Mobile	No Limit
✎ ✕	TOC Only	Documentation Domain	For TOC only access in EOC	30 min

Displaying items 1 - 6 of 6

Figure 75 — Group Details Screen

(2) Press the **Delete Icon** (red X) next to the user whose attributes you want to edit and you will see the screen shown in Figure 76.



Message from webpage

Delete item?

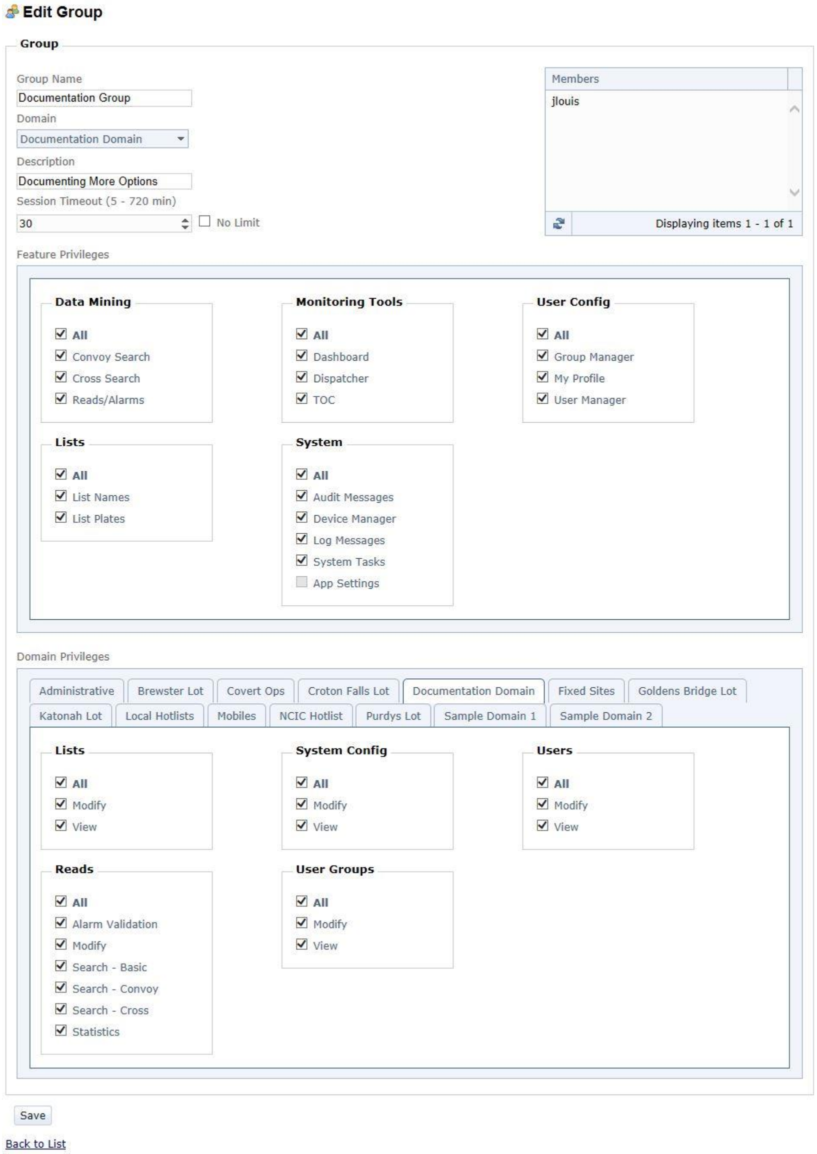
Figure 76 — Delete Group Confirmation

(3) Press **OK**. The group is deleted from the system.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Group Manager Privileges Examples

The Documentation Group Permissions set are shown below in Figure 77.



Edit Group

Group

Group Name: Documentation Group
Domain: Documentation Domain
Description: Documenting More Options
Session Timeout (5 - 720 min): 30 □ No Limit

Members: jlouis
Displaying items 1 - 1 of 1

Feature Privileges

Data Mining
☑ All
☑ Convoy Search
☑ Cross Search
☑ Reads/Alarms

Monitoring Tools
☑ All
☑ Dashboard
☑ Dispatcher
☑ TOC

User Config
☑ All
☑ Group Manager
☑ My Profile
☑ User Manager

Lists
☑ All
☑ List Names
☑ List Plates

System
☑ All
☑ Audit Messages
☑ Device Manager
☑ Log Messages
☑ System Tasks
□ App Settings

Domain Privileges

Administrative | Brewster Lot | Covert Ops | Croton Falls Lot | Documentation Domain | Fixed Sites | Goldens Bridge Lot | Katonah Lot | Local Hotlists | Mobiles | NCIC Hotlist | Purdys Lot | Sample Domain 1 | Sample Domain 2

Lists
☑ All
☑ Modify
☑ View

System Config
☑ All
☑ Modify
☑ View

Users
☑ All
☑ Modify
☑ View

Reads
☑ All
☑ Alarm Validation
☑ Modify
☑ Search - Basic
☑ Search - Convoy
☑ Search - Cross
☑ Statistics

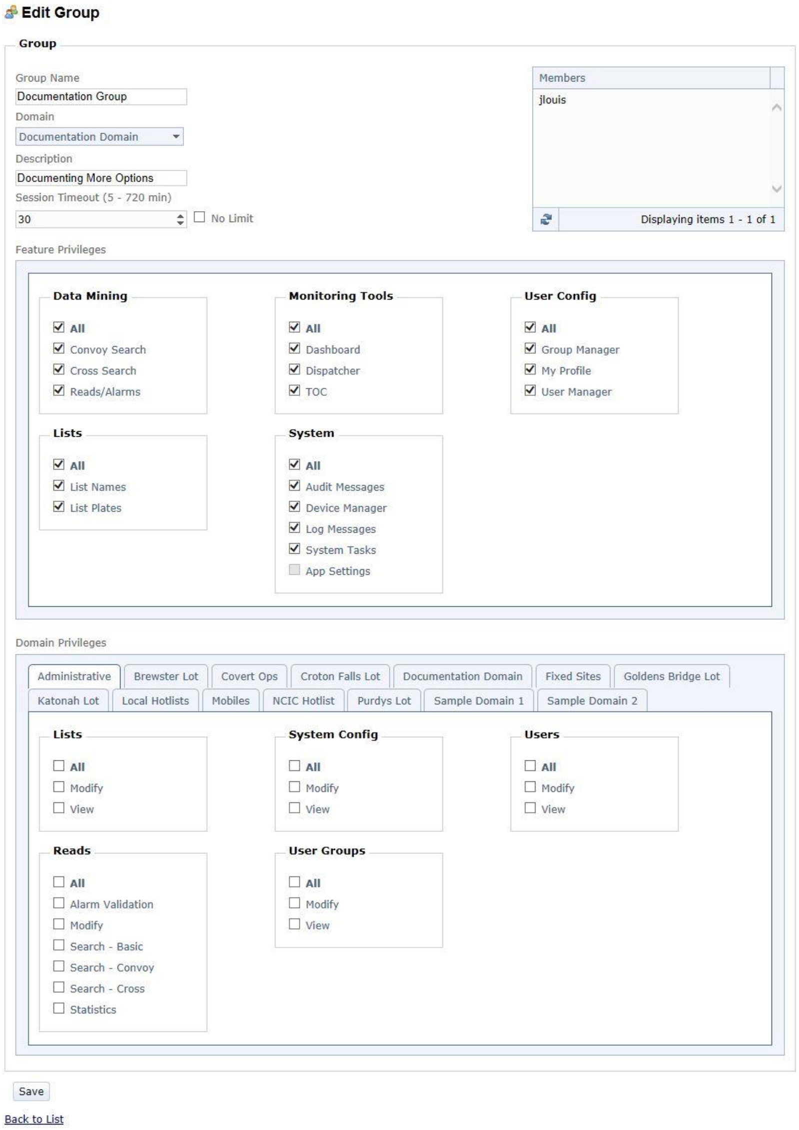
User Groups
☑ All
☑ Modify
☑ View

Figure 77 — Group Permissions Set

Referring to Figure 77, notice that the group **Documentation** has full access to all areas of the EOC based on the **Feature Privileges** selected and for the selected **Documentation** Domain.

In this case, a user account that is only a member of the **Documentation** group can view, search or modify list data, see read data in all search possibilities, create and view other users, perform system configuration tasks, as well as view, create and edit user groups. All these permissions apply to the **Documentation** domain only (the selected tab under Domain Privileges). You can also see a list of the group's members in the upper right.

NOTE: Referring to Figure 78, in a different domain, say **Administrative**, the **Documentation** group has no Domain Privileges at all. This means that a user account associated only with the **Documentation** group cannot view read data from any devices associated with the **Administrative** domain. In fact, a user account only associated with the **Documentation** group will not even see the **Administrative** domain when they log into the EOC.



Edit Group

Group

Group Name: Documentation Group

Domain: Documentation Domain

Description: Documenting More Options

Session Timeout (5 - 720 min): 30 □ No Limit

Members: jlouis

Displaying items 1 - 1 of 1

Feature Privileges

Data Mining
- ☑ All
- ☑ Convoy Search
- ☑ Cross Search
- ☑ Reads/Alarms

Monitoring Tools
- ☑ All
- ☑ Dashboard
- ☑ Dispatcher
- ☑ TOC

User Config
- ☑ All
- ☑ Group Manager
- ☑ My Profile
- ☑ User Manager

Lists
- ☑ All
- ☑ List Names
- ☑ List Plates

System
- ☑ All
- ☑ Audit Messages
- ☑ Device Manager
- ☑ Log Messages
- ☑ System Tasks
- □ App Settings

Domain Privileges

Lists
- □ All
- □ Modify
- □ View

System Config
- □ All
- □ Modify
- □ View

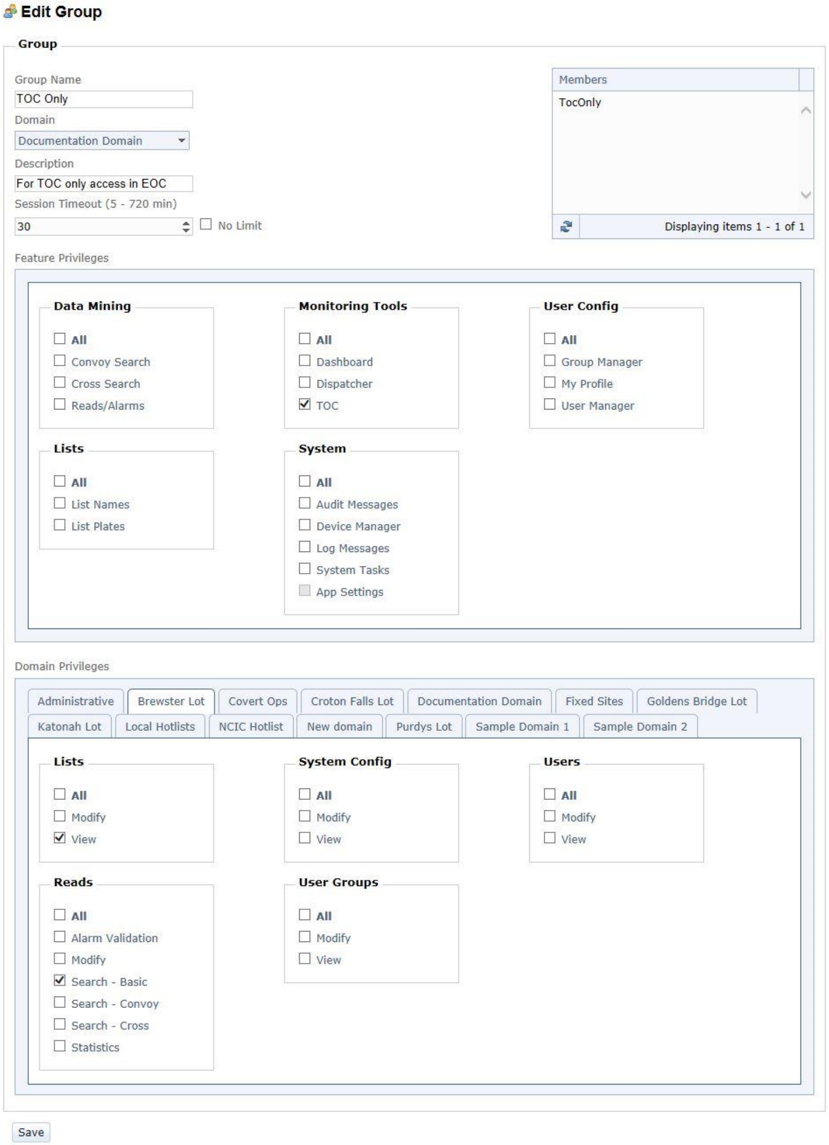
Users
- □ All
- □ Modify
- □ View

Reads
- □ All
- □ Alarm Validation
- □ Modify
- □ Search - Basic
- □ Search - Convoy
- □ Search - Cross
- □ Statistics

User Groups
- □ All
- □ Modify
- □ View

Figure 78 — Group Permissions Not Set

NOTE: Referring to Figure 79 below, the **TOC Only** group only has EOC **Feature Privileges** to **TOC** for the domain **Brewster Lot** (all other domains have no enabled privileges). This means that a user account associated with the **TOC Only** group only has access to the EOC for running TOC and can only see alarm data from **Brewster Lot**. In fact, a user account associated with the **TOC Only** group will not even see any of the other EOC Menu options or domains when it logs into the EOC.



Edit Group

Group

Group Name: TOC Only

Domain: Documentation Domain

Description: For TOC only access in EOC

Session Timeout (5 - 720 min): 30 □ No Limit

Members: TocOnly

Displaying items 1 - 1 of 1

Feature Privileges

Data Mining: □ All □ Convoy Search □ Cross Search □ Reads/Alarms

Monitoring Tools: □ All □ Dashboard □ Dispatcher ☑ TOC

User Config: □ All □ Group Manager □ My Profile □ User Manager

Lists: □ All □ List Names □ List Plates

System: □ All □ Audit Messages □ Device Manager □ Log Messages □ System Tasks □ App Settings

Domain Privileges

Administrative | Brewster Lot | Covert Ops | Croton Falls Lot | Documentation Domain | Fixed Sites | Goldens Bridge Lot | Katonah Lot | Local Hotlists | NCIC Hotlist | New domain | Purdys Lot | Sample Domain 1 | Sample Domain 2

Lists: □ All □ Modify ☑ View

System Config: □ All □ Modify □ View

Users: □ All □ Modify □ View

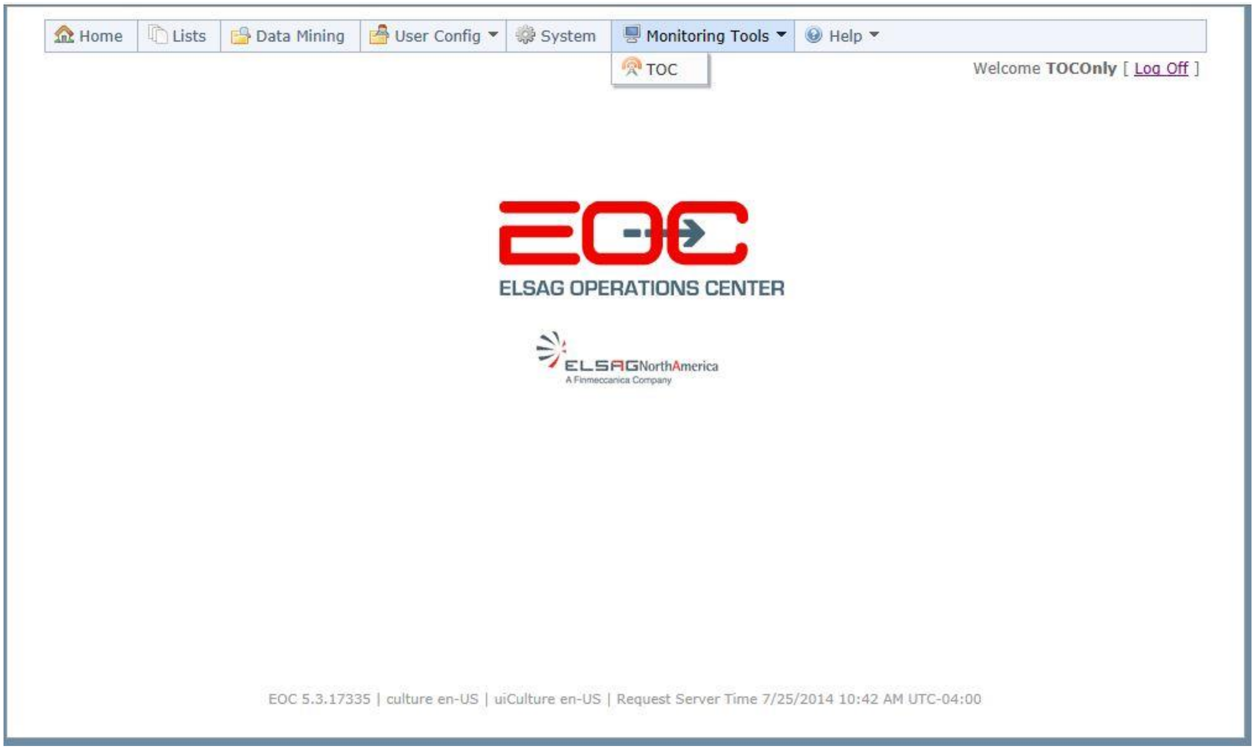
Reads: □ All □ Alarm Validation □ Modify ☑ Search - Basic □ Search - Convoy □ Search - Cross □ Statistics

User Groups: □ All □ Modify □ View

Save

Figure 79 — Group Permissions Feature Restricted

Referring to Figure 80, this is an example of what a **TOC Only** group user would see when logged into EOC. The user only has access under **User Config** to change their password and under **Monitoring Tools** access to **TOC**.



EOC 5.3.17335 | culture en-US | uiCulture en-US | Request Server Time 7/25/2014 10:42 AM UTC-04:00

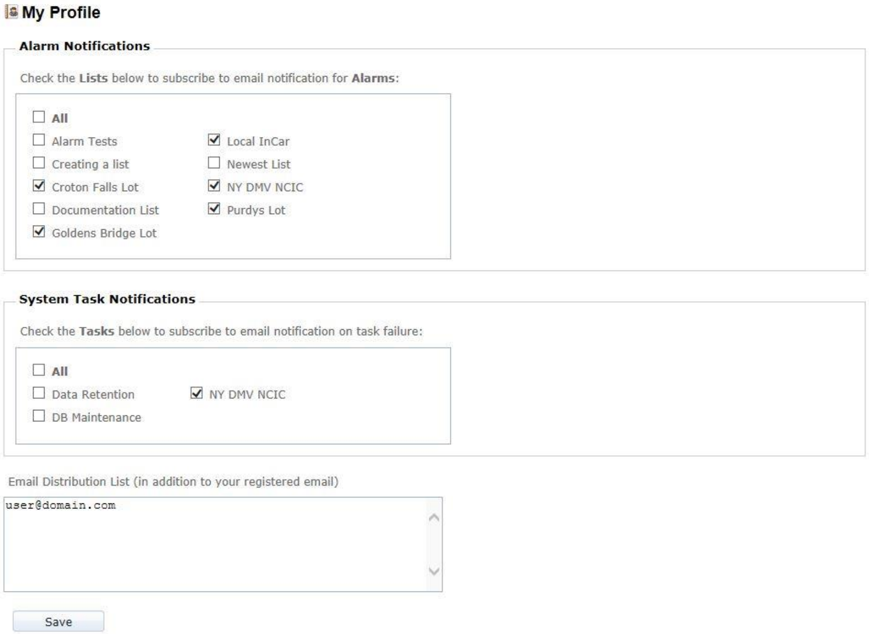
Figure 80 — Group Permissions TOC Only Example

Create a Profile

The EOC allows you to create a per-user profile that controls various aspects of how that user interacts with the system. The profile controls whether a user receives an email when an alarm sounds against a list or lists or when a System Task has failed. To create a profile, refer to Figure 81 and perform the steps that follow:

(1) To create a profile, log in as the user you want to receive emails.

(2) Select **User Config > My Profile** from the main menu.



My Profile

Alarm Notifications

Check the **Lists** below to subscribe to email notification for **Alarms**:

☐ **All**
☐ Alarm Tests
☐ Creating a list
☑ Croton Falls Lot
☐ Documentation List
☑ Goldens Bridge Lot
☑ Local InCar
☐ Newest List
☑ NY DMV NCIC
☑ Purdys Lot

System Task Notifications

Check the **Tasks** below to subscribe to email notification on task failure:

☐ **All**
☐ Data Retention
☐ DB Maintenance
☑ NY DMV NCIC

Email Distribution List (in addition to your registered email)

```
user@domain.com
```

Figure 81 — My Profile Screen

(3) Select the list or lists you want to receive email notifications for when an alarm is generated.

(4) Select the System Task or tasks you want to receive email notifications for when a task fails to complete successfully.

(5) Press **Save**.

NOTE: Email Distribution List allows for duplicate emails to be sent to other email addresses or email distribution lists. This allows an email alert to be sent to someone who does not have access to the EOC. Use a comma to separate email addresses.

Chapter 6 — Lists

Introduction

The EOC allows you to manage lists, which are collections of license plate data associated with illegal activity. You can manage the lists and their attributes and upload existing list data through the EOC. Script files (XML) parse the incoming data into a correct format for the DB

Use **List Names** and **List Plates** selections to search, view, and edit the data in the lists themselves.

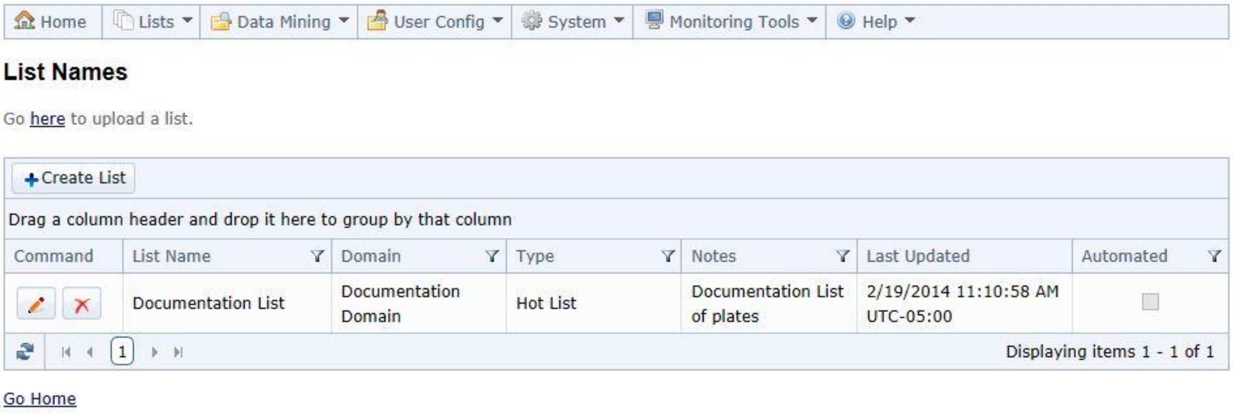
List Names

The List Names functionality allows you to create, edit, delete and view list characteristics.

Creating a List

Referring to Figure 82, to create a new List, select **Lists > List Names** from the menu at the top of the page. You will see a display of the lists in the system.

> **NOTE:** You will only see Lists you have access to see (there is nothing grayed out).



List Names

Go here to upload a list.

Drag a column header and drop it here to group by that column

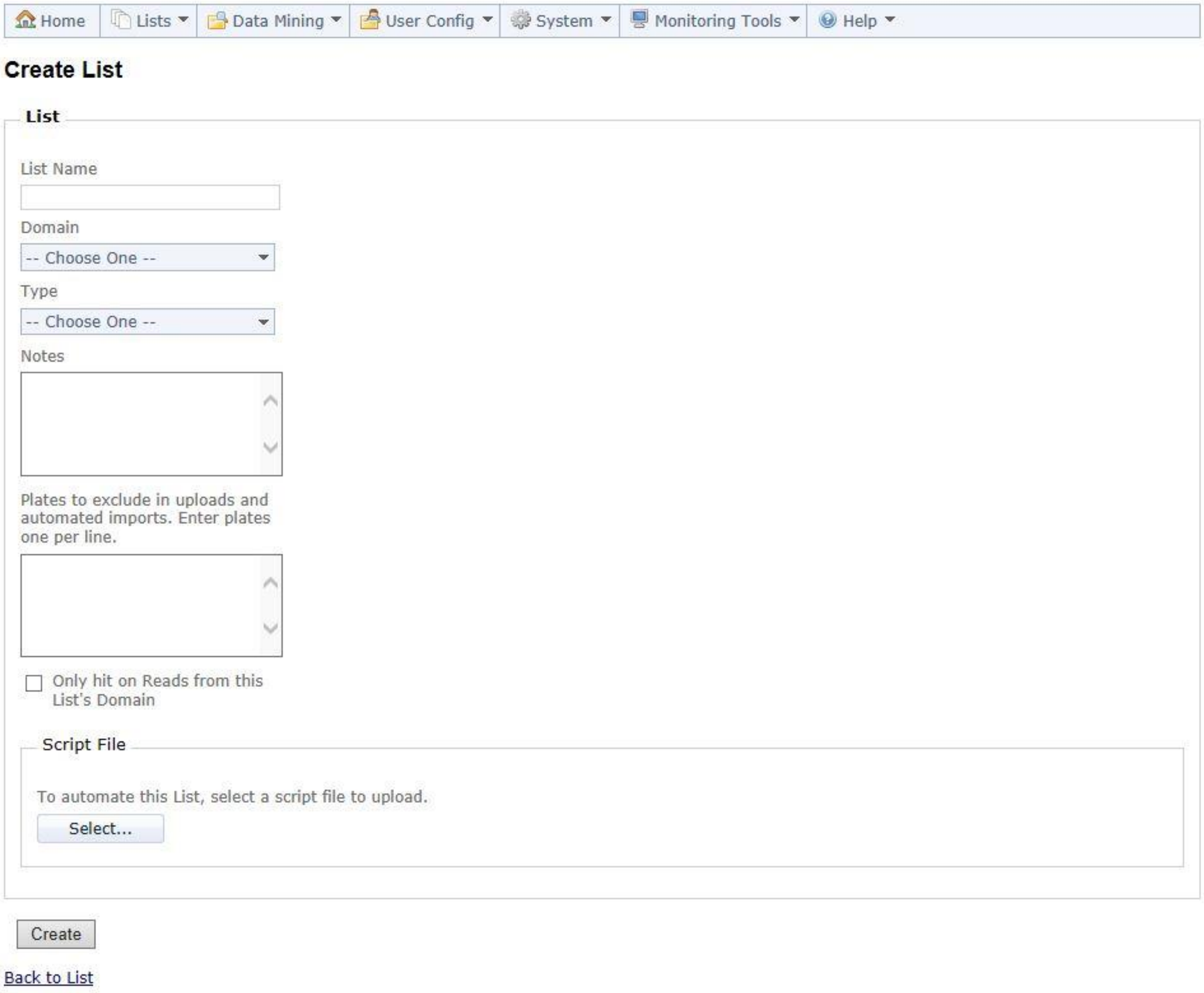
Command	List Name	Domain	Type	Notes	Last Updated	Automated
✎ ✗	Documentation List	Documentation Domain	Hot List	Documentation List of plates	2/19/2014 11:10:58 AM UTC-05:00	□

Displaying items 1 - 1 of 1

Go Home

Figure 82 — List Initial Screen

Press the "+ Create List" button and the screen shown in Figure 83 will appear.



Create List

List

List Name

Domain

-- Choose One --

Type

-- Choose One --

Notes

Plates to exclude in uploads and automated imports. Enter plates one per line.

☐ Only hit on Reads from this List's Domain

Script File

To automate this List, select a script file to upload.

Figure 83 — Create List Screen

Fill in the following information about the list:

- List Name — Type in the name of the list.
- Domain — Select the EOC domain in which you want to create this list. You will only see domains to which you have access, and
- Type — The type of list
  - Hot List
  - White List*
- Notes — Type in any notes about the list that are pertinent
- Plates to exclude in uploads and automated imports (enter plates one per line)

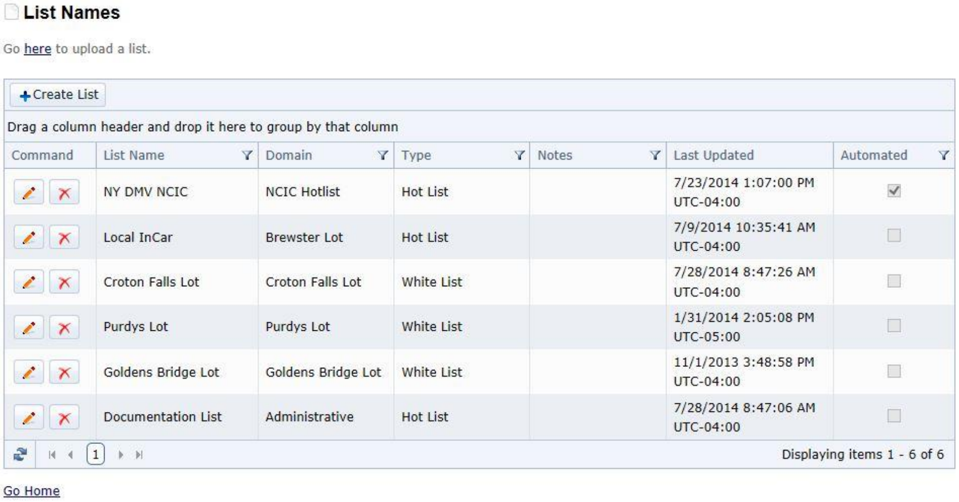
- "Only hit on Reads from this List's Domain" checkbox. This option MUST be selected and is only for White List* use.
- Script File — Press **Select** to choose the XML file that will defines where to find the incoming data file or source for the automated list import. You will get a Windows selection menu that lets you navigate to the appropriate script file, and

Press **Create** to create the List structure for this List.

> *** NOTE:** White List is a list of authorized plates for a location such as a parking lot with authorized parkers. Alarms will sound on plates that are NOT in the White List.

Viewing List Names

To view List Names, select **Lists > List Names** from the menu at the top of the page. As shown in Figure 84, you will see a display of the lists in the system you have permission to view.



List Names

Go here to upload a list.

+Create List

Drag a column header and drop it here to group by that column

Command	List Name	Domain	Type	Notes	Last Updated	Automated
✎ ✕	NY DMV NCIC	NCIC Hotlist	Hot List		7/23/2014 1:07:00 PM UTC-04:00	☑
✎ ✕	Local InCar	Brewster Lot	Hot List		7/9/2014 10:35:41 AM UTC-04:00	☐
✎ ✕	Croton Falls Lot	Croton Falls Lot	White List		7/28/2014 8:47:26 AM UTC-04:00	☐
✎ ✕	Purdys Lot	Purdys Lot	White List		1/31/2014 2:05:08 PM UTC-05:00	☐
✎ ✕	Goldens Bridge Lot	Goldens Bridge Lot	White List		11/1/2013 3:48:58 PM UTC-04:00	☐
✎ ✕	Documentation List	Administrative	Hot List		7/28/2014 8:47:06 AM UTC-04:00	☐

Displaying items 1 - 6 of 6

Go Home

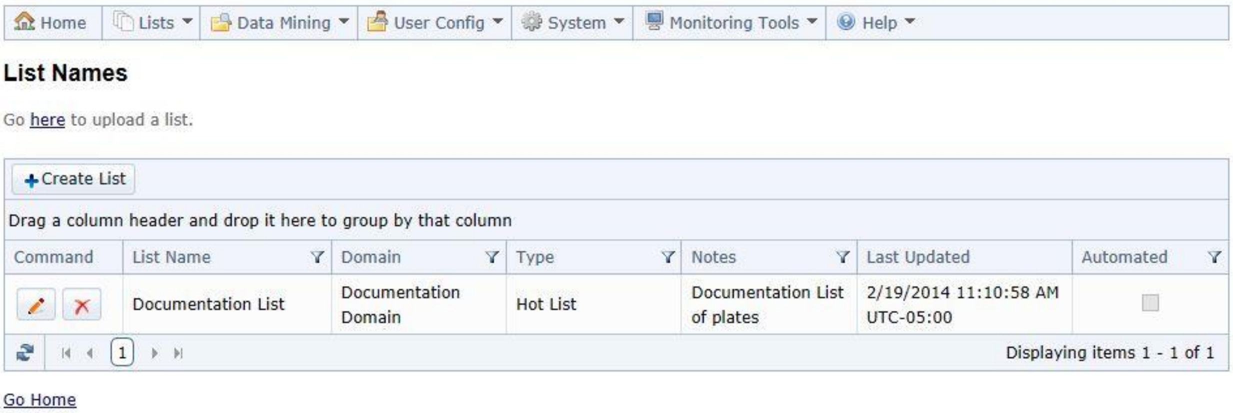
Figure 84 — Existing Lists

You can easily view in this display the following information about the lists you have access to:

- **List Name** — Name of the list
- **Domain** — The EOC domain of this list
- **Type** — The type of list:
  - Hot List
  - White List
- **Notes** — Any pertinent notes about the list
- **Last Updated** — Last date and time the list was updated.

Editing a List

To edit a List, select **Lists > List Names** from the menu at the top of the page. You will see a display of the lists in the system. (Lists you do not have permission to view are not visible.) See Figure 85.



List Names

Go here to upload a list.

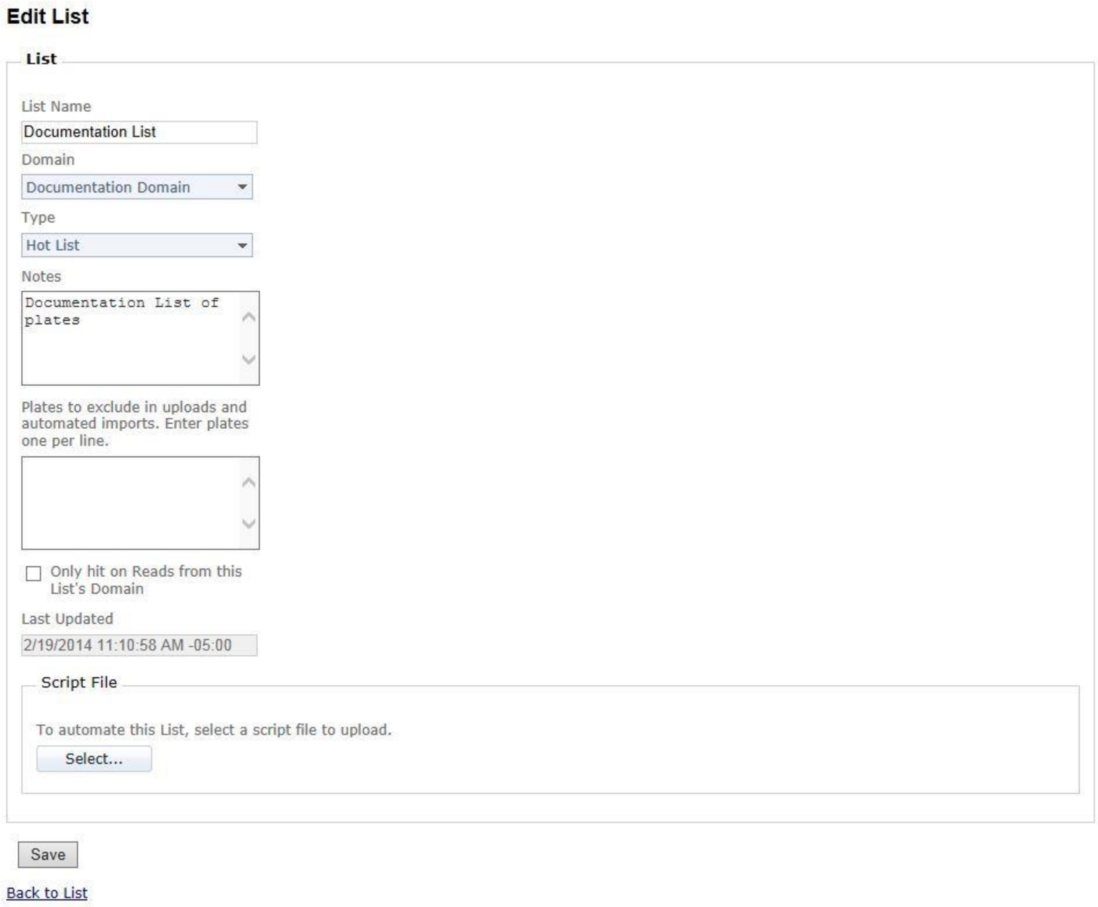
Drag a column header and drop it here to group by that column

Command	List Name	Domain	Type	Notes	Last Updated	Automated
	Documentation List	Documentation Domain	Hot List	Documentation List of plates	2/19/2014 11:10:58 AM UTC-05:00	□

Displaying items 1 - 1 of 1

Figure 85 — Existing Lists to Edit

Press the **Edit** (Pencil Icon) button next to the list you want to edit, which opens up the **Edit List** screen (see Figure 86).



Edit List

List

List Name: Documentation List

Domain: Documentation Domain

Type: Hot List

Notes: Documentation List of plates

Plates to exclude in uploads and automated imports. Enter plates one per line.

□ Only hit on Reads from this List's Domain

Last Updated: 2/19/2014 11:10:58 AM -05:00

Script File

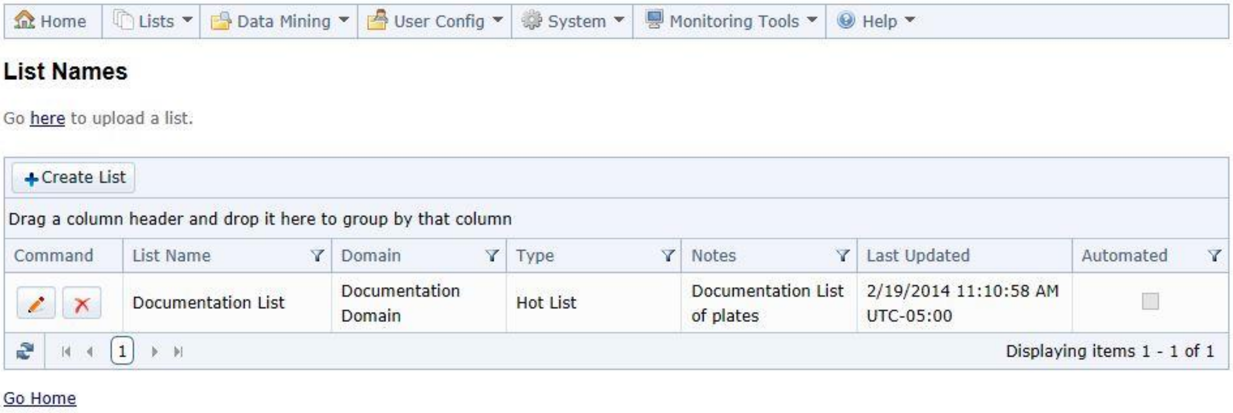
To automate this List, select a script file to upload.

Figure 86 — Edit List Screen

Change whatever information about the list you want and then press **Save** to save your changes.

Deleting a List

Referring to Figure 87, to delete a List, select **Lists > List Names** from the menu at the top of the page. You will see a display of the existing lists in the system.



List Names

Go here to upload a list.

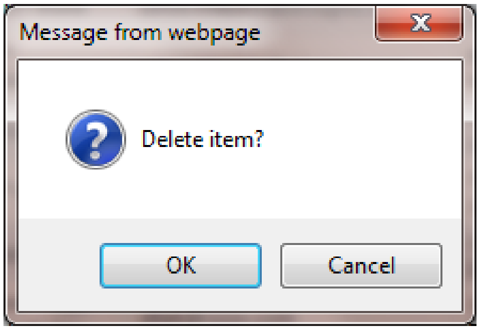
Drag a column header and drop it here to group by that column

Command	List Name	Domain	Type	Notes	Last Updated	Automated
	Documentation List	Documentation Domain	Hot List	Documentation List of plates	2/19/2014 11:10:58 AM UTC-05:00	□

1 Displaying items 1 - 1 of 1

Figure 87 — Existing Lists

Press the **Delete** (Red X) button next to the list you want to delete. You will be prompted to verify the deletion as shown in Figure 88.



Delete item?

Figure 88 — Delete List Confirmation

Press **OK** to delete the list. The delete operation deletes both the EOC List structure that you created and any data in that list.

Importing Data into the EOC

❑ List Data

List data can be imported into the EOC from external sources. A utility installed with the system uses the script information you associated with the EOC list structure above to parse the incoming data into a format suitable for the EOC's database. The utility can be configured to run automatically at a time of day when there is less pressure on the EOC system, so as to minimize any effects on response time. For information about importing list data, see the *List Upload* section on Page 106.

NOTE: We recommend that the total list entries for all lists does not exceed 6 million records.

❑ List Data from CarSystem

List data from CarSystem is automatically entered in the EOC.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Searching for a Plate in a List

To search for a plate in a list perform the following steps:

(1) First select **Lists > List Plates** from the menu at the top of the page and the screen in Figure 89 will appear.

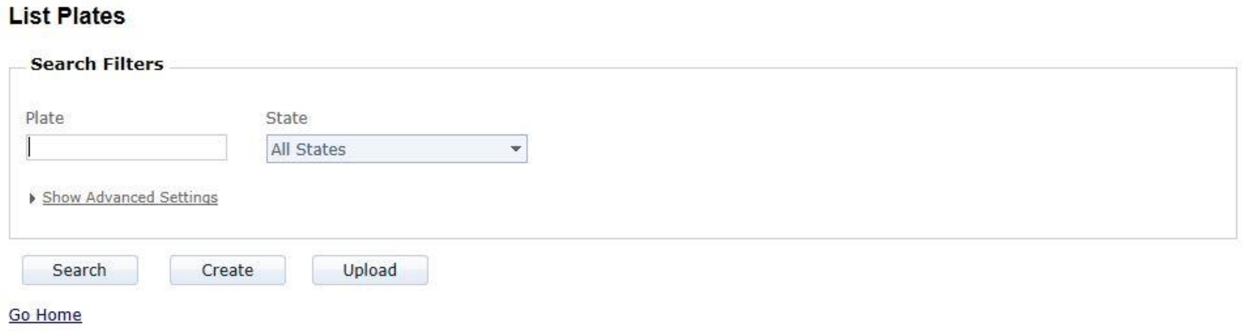
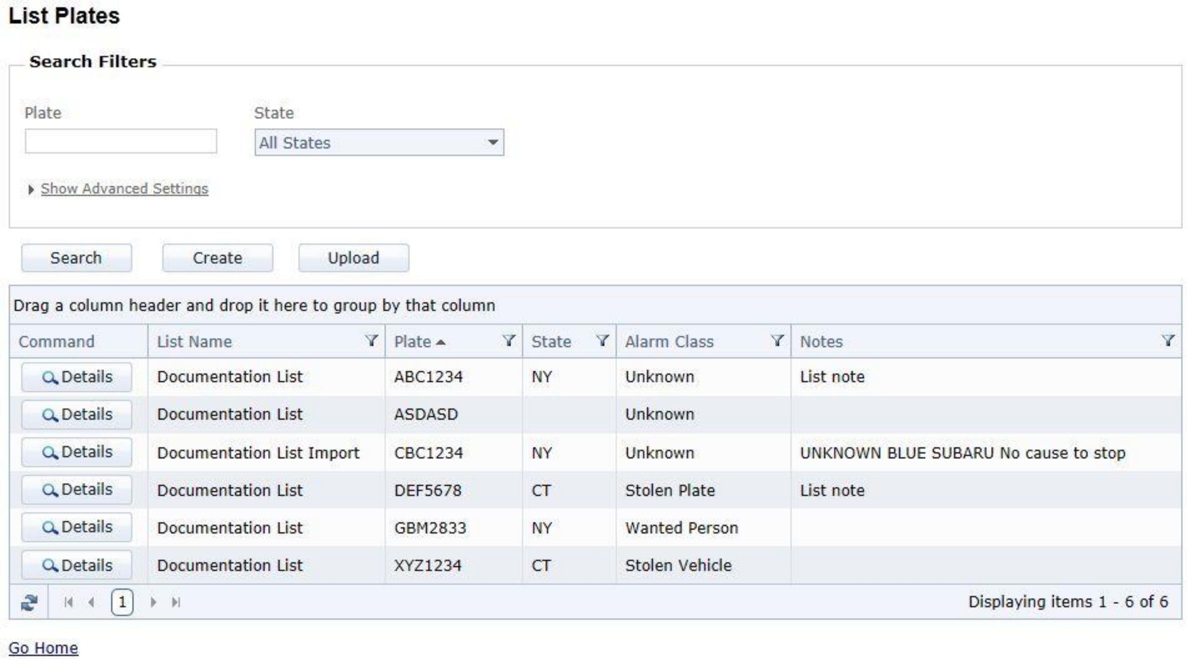


Figure 89 — Search List Plates Screen

(2) Press the **Search** button. Referring to Figure 90, you will see a record of all the plates in the system. **NOTE**: you will only see plates in Lists that you have permission to view.



Command	List Name	Plate ▲	State	Alarm Class	Notes
Details	Documentation List	ABC1234	NY	Unknown	List note
Details	Documentation List	ASDASD		Unknown	
Details	Documentation List Import	CBC1234	NY	Unknown	UNKNOWN BLUE SUBARU No cause to stop
Details	Documentation List	DEF5678	CT	Stolen Plate	List note
Details	Documentation List	GBM2833	NY	Wanted Person	
Details	Documentation List	XYZ1234	CT	Stolen Vehicle	

1 Displaying items 1 - 6 of 6

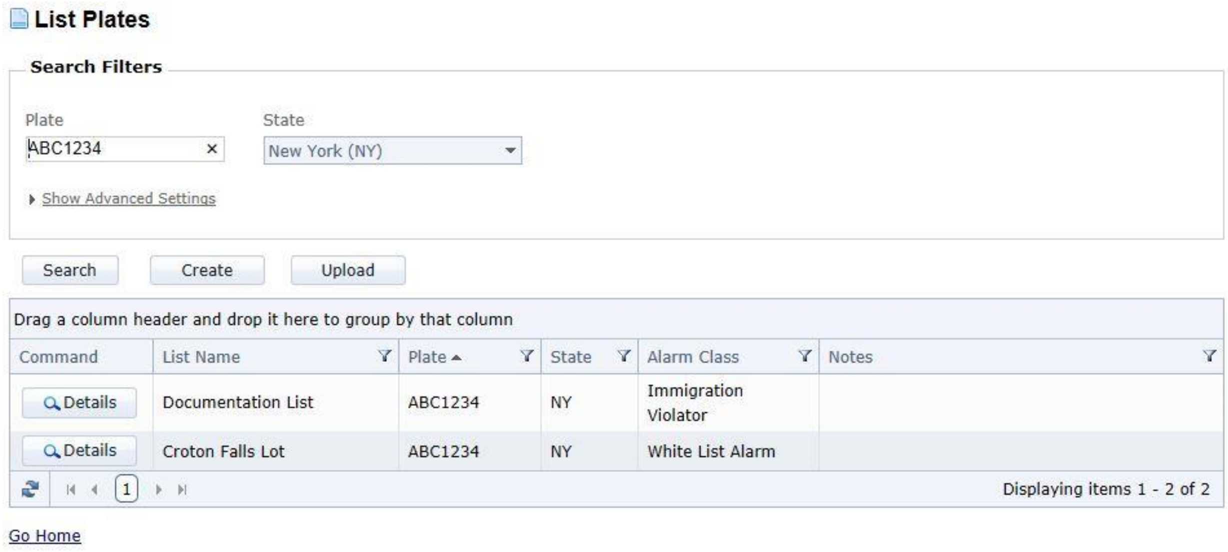
Figure 90 — List Plates Search Results

(3) Referring to Figure 91, type in the **Plate Number** you are searching for and select the **State** from the drop down and press **Search**.

NOTE: If you know that the plate is associated with a certain **Alarm Class**, press **Show Advanced Settings** and deselect all the Alarm Classes except the one you know is associated with the plate. This will speed the search.

NOTE: You can also use Advanced Settings to limit the search to certain lists and to show expired list entries, which are not displayed by default.

NOTE: In this sample result, the same plate was found in two lists.



List Plates

Search Filters

Plate: ABC1234

State: New York (NY)

Drag a column header and drop it here to group by that column

Command	List Name	Plate ▲	State	Alarm Class	Notes
Details	Documentation List	ABC1234	NY	Immigration Violator	
Details	Croton Falls Lot	ABC1234	NY	White List Alarm	

Displaying items 1 - 2 of 2

Figure 91 — List Plates Search Screen Results

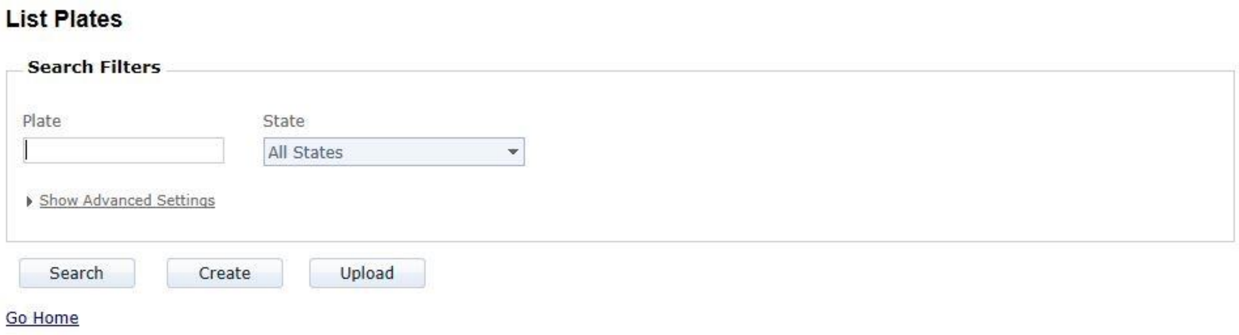
Managing List Plates

Use the **List Plates** selection from the menu to add, view, edit, and delete individual plates from a list.

Add a Plate to a List

To add a plate to a List perform the following steps:

(1) Select **Lists > List Plates** from the menu at the top of the page. You will see the search screen shown in Figure 92.



List Plates

Search Filters

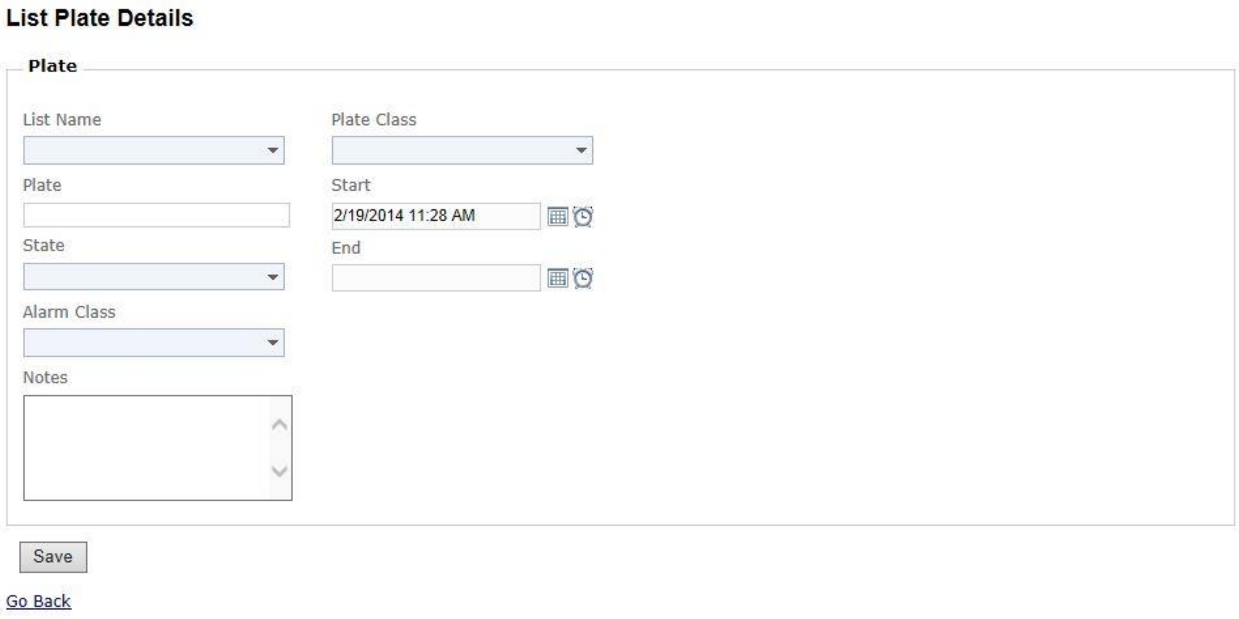
Plate

State

All States

Figure 92 — Manage List Plates Screen

(2) Press the **Create** button to add a plate. You will see the screen shown in Figure 93.



List Plate Details

Plate

List Name

Plate Class

Plate

Start

2/19/2014 11:28 AM

State

End

Alarm Class

Notes

Figure 93 — Create List Plate Details Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(3) Enter the following information:

- **List Name** — From the drop down menu
- **Plate** — Type in the plate number
- **State** — Select a state from the drop down
- **Alarm Class** — Select an alarm class from the drop down
- **Notes** — Type in any notes about the list that are pertinent
- **Plate Class** (not required), and
- **Start** and **End Date** and **Time** — The interval for which the list entry is valid. Start Time is defaulted to the entry time. End Time is not required and can be entered later.

(4) Press **Save** to create the List plate entry.

View or Edit a Plate in a List

You may need to change information about a plate in a list, to either update information, add notes or otherwise correct the information.

Before you can view, edit or delete a plate from a list, you must search for it. The search process is identical to that outlined in other sections. To view or edit a plate in a list perform the steps that follow:

(1) First select **Lists > List Plates** from the menu at the top of the page and the screen shown below in Figure 94 will appear.

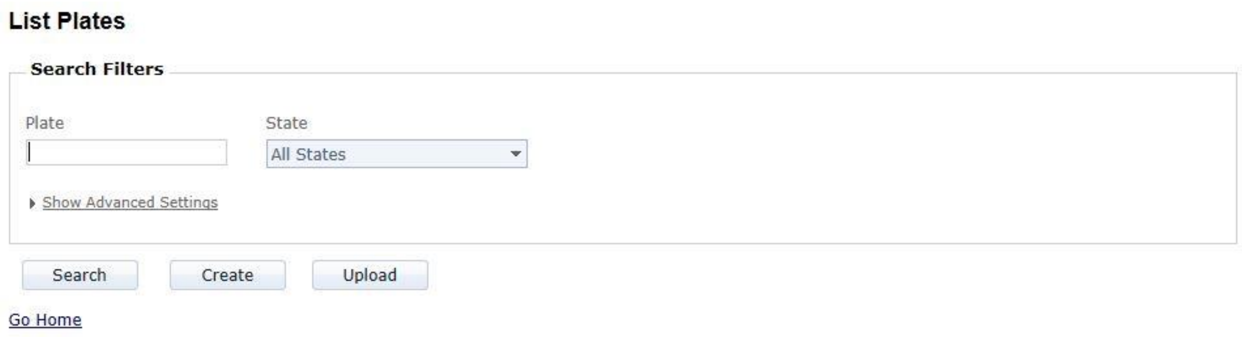
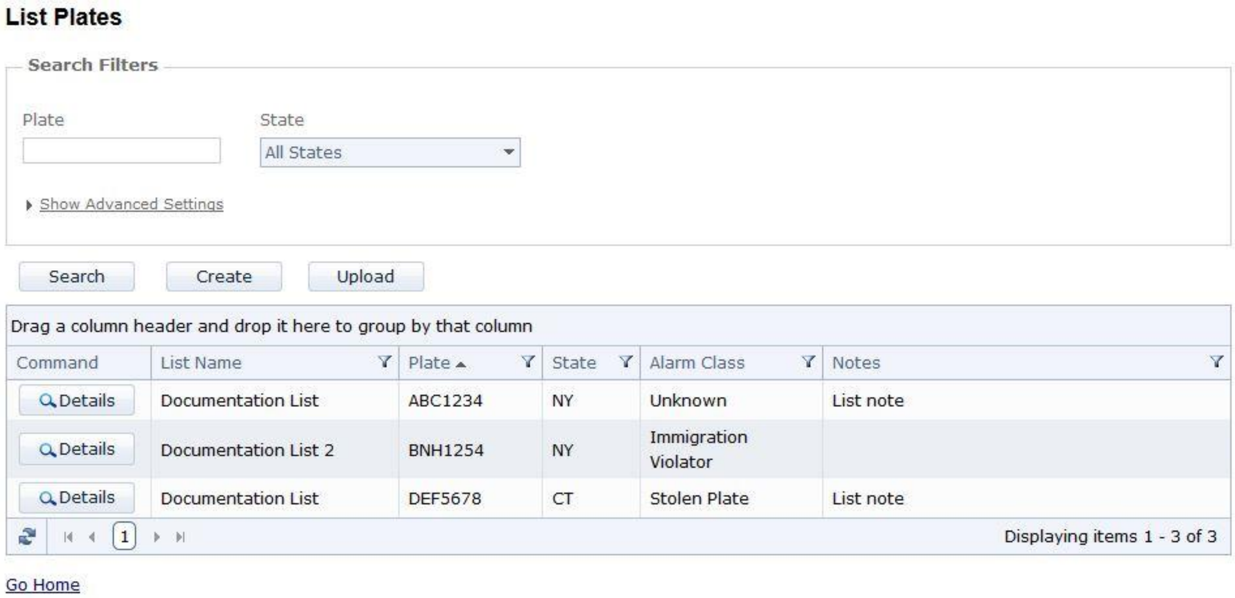


Figure 94 — List Plates Search Filters

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(2) Press the **Search** button. You will see a record of the plates in the system. Referring to Figure 95, you will only see plates in lists that you have permission to view.



List Plates

Search Filters

Plate

State: All States

▸ Show Advanced Settings

Search
Create
Upload
Drag a column header and drop it here to group by that column

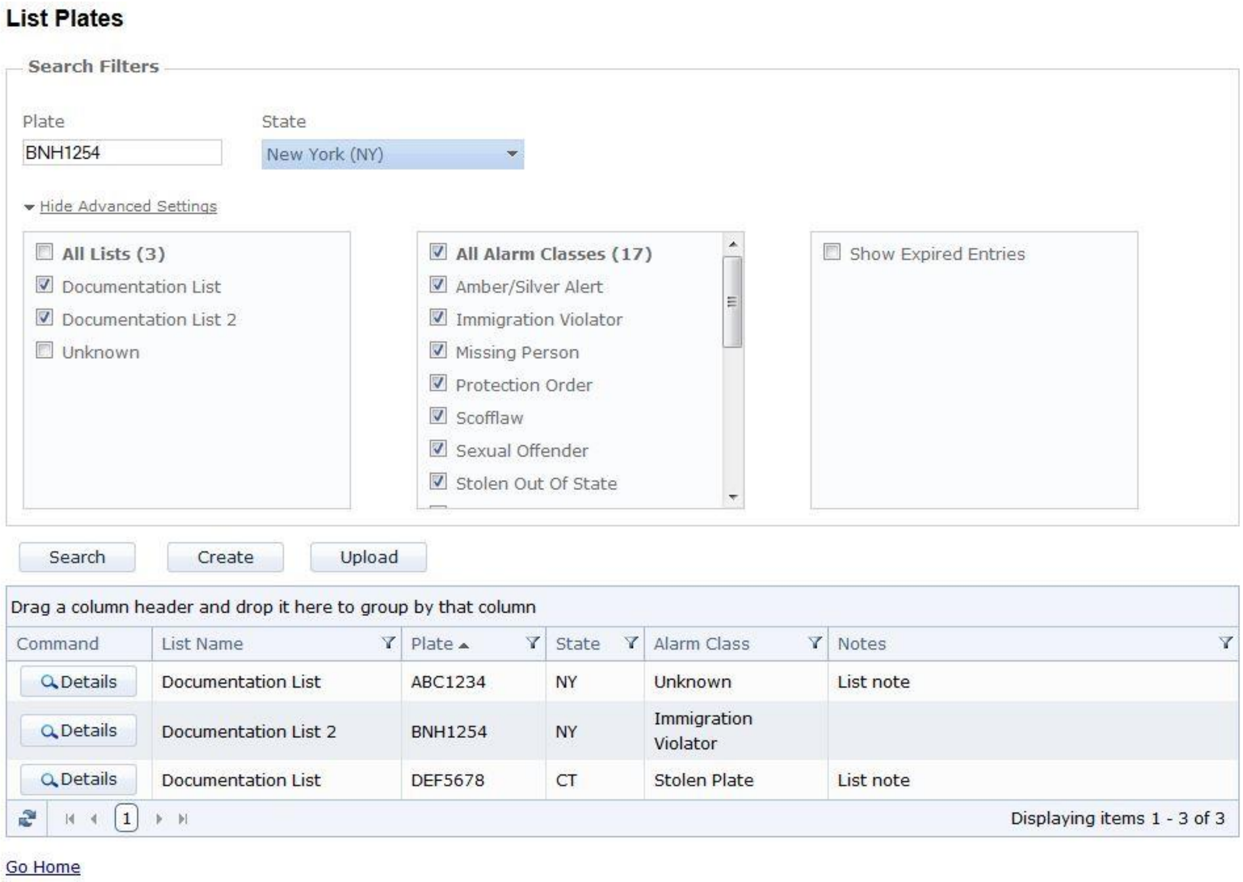
Command	List Name	Plate ▲	State	Alarm Class	Notes
Details	Documentation List	ABC1234	NY	Unknown	List note
Details	Documentation List 2	BNH1254	NY	Immigration Violator	
Details	Documentation List	DEF5678	CT	Stolen Plate	List note

1
Displaying items 1 - 3 of 3
Go Home

Figure 95 — List Plates Search Screen

(3) Referring to Figure 96, type in the **Plate Number** you want to view or edit and select the **State** from the drop down menu.

NOTE: If you know that the plate is associated with a certain **Alarm Class**, press **Show Advanced Settings** and deselect all Alarm Classes except the one you know is associated with the plate. This will speed the search. You can also filter the search to specific lists and/or search expired lists for the plate as well.



List Plates

Search Filters

Plate: BNH1254

State: New York (NY)

▾ Hide Advanced Settings

☐ All Lists (3)
☑ Documentation List
☑ Documentation List 2
☐ Unknown

☑ All Alarm Classes (17)
☑ Amber/Silver Alert
☑ Immigration Violator
☑ Missing Person
☑ Protection Order
☑ Scofflaw
☑ Sexual Offender
☑ Stolen Out Of State

☐ Show Expired Entries

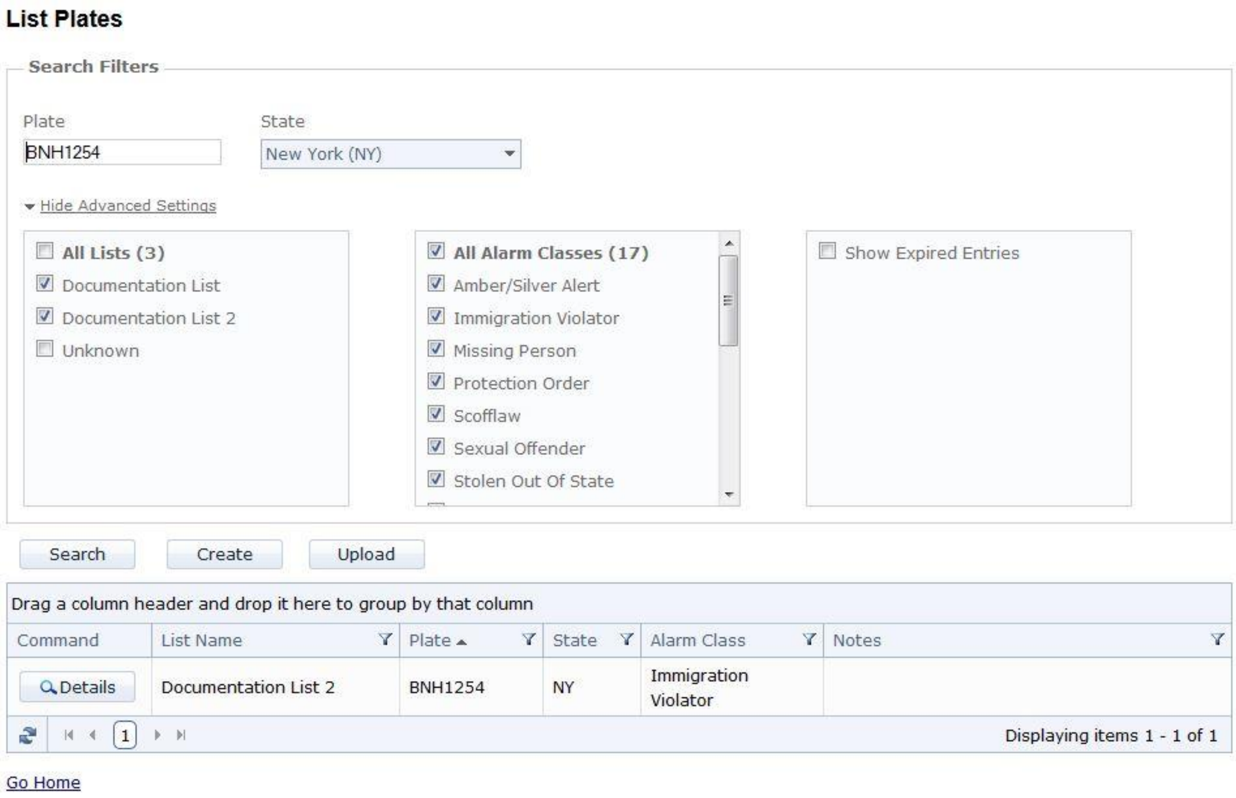
Search
Create
Upload
Drag a column header and drop it here to group by that column

Command	List Name	Plate ▴	State	Alarm Class	Notes
Details	Documentation List	ABC1234	NY	Unknown	List note
Details	Documentation List 2	BNH1254	NY	Immigration Violator	
Details	Documentation List	DEF5678	CT	Stolen Plate	List note

Displaying items 1 - 3 of 3

Figure 96 — List Plates Search Screen (Parameters Added)

(4) Press **Search** and a screen similar to the one shown in Figure 97 will appear.



List Plates

Search Filters

Plate: BNH1254

State: New York (NY)

Hide Advanced Settings

☐ All Lists (3)
☑ Documentation List
☑ Documentation List 2
☐ Unknown

☑ All Alarm Classes (17)
☑ Amber/Silver Alert
☑ Immigration Violator
☑ Missing Person
☑ Protection Order
☑ Scofflaw
☑ Sexual Offender
☑ Stolen Out Of State

☐ Show Expired Entries

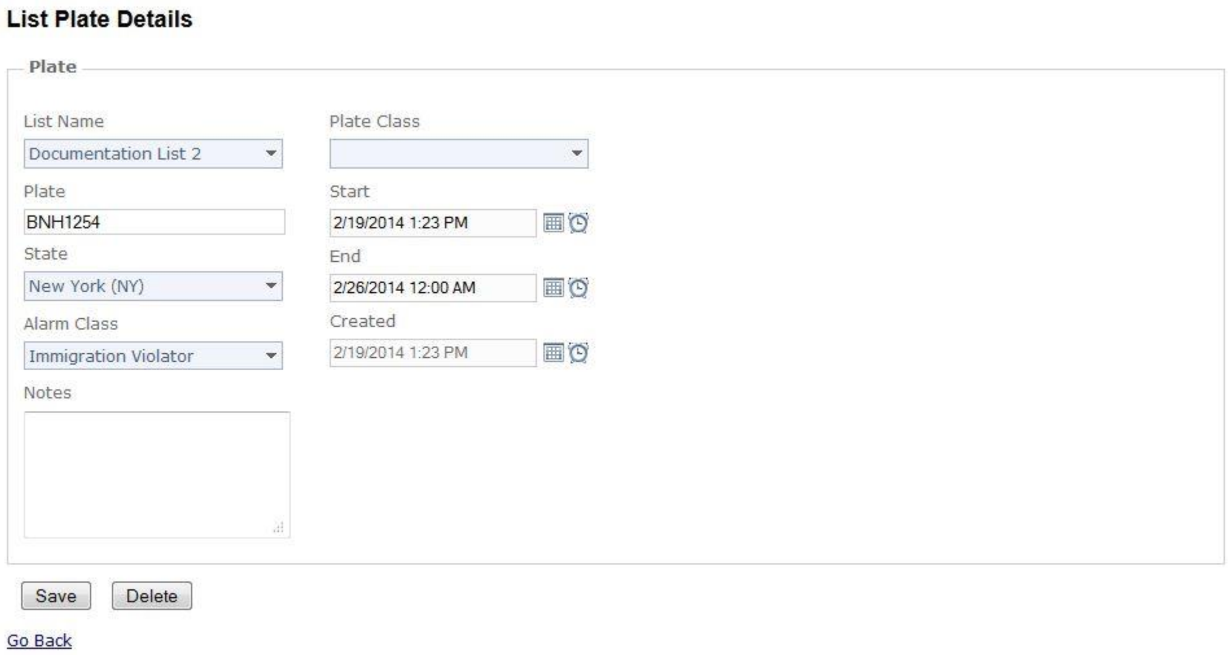
Search
Create
Upload
Drag a column header and drop it here to group by that column

Command	List Name	Plate	State	Alarm Class	Notes
Details	Documentation List 2	BNH1254	NY	Immigration Violator	

Displaying items 1 - 1 of 1

Figure 97 — List Plates Search Results

(5) Press the **Details** button next to the plate you are interested in and a screen similar to the one shown in Figure 98 will appear.



List Plate Details

Plate

List Name: Documentation List 2

Plate Class:

Plate: BNH1254

Start: 2/19/2014 1:23 PM

State: New York (NY)

End: 2/26/2014 12:00 AM

Alarm Class: Immigration Violator

Created: 2/19/2014 1:23 PM

Notes:

Figure 98 — List Plates Details

(6) Edit whatever details you need to edit and then press **Save** to save your changes.

NOTE: If the **Save** button or any information in any field is grayed out, you will be unable to edit this plate.

Delete a Plate from a List

You may need to delete a plate that is in a list.

Before you can delete an individual plate, you must search for it. The search process is identical to that outlined earlier in this section so refer to those figures if clarification is needed.

(1) First, select **Lists > List Plates** from the menu at the top of the page.

(2) Type in the **Plate Number** you want to delete and select the **State** from the drop down.

NOTE: If you know that the plate is associated with a certain **Alarm Class**, press **Show Advanced Settings** and deselect all Alarm Classes except the one you know is associated with the plate. This will speed the search. You can also filter the search to specific lists and/or search expired lists for the plate as well.

(3) Press **Search**.

(4) Review the results and then press the **Details** button next to the plate of interest.

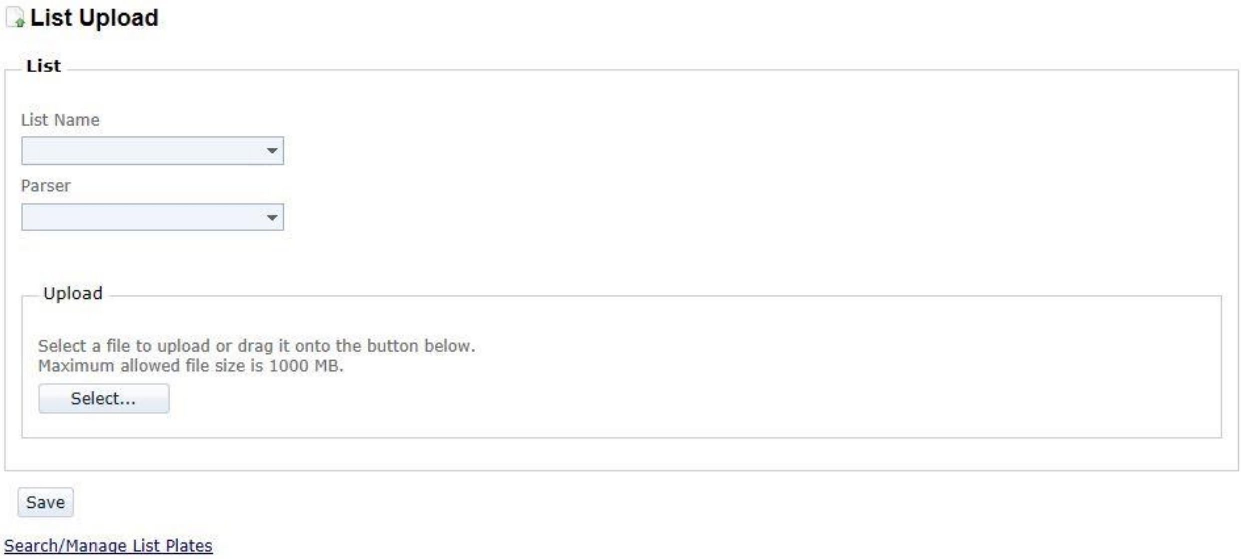
(5) Press **Delete** to delete the plate.

NOTE: If the Delete button is grayed out, you do not have permissions to delete a List plate.

List Upload

You can upload a fresh copy of a list's data. To do this, perform the steps that follow:

(1) Select **Lists > List Upload** from the menu at the top of the page and the screen shown in Figure 99 will appear.

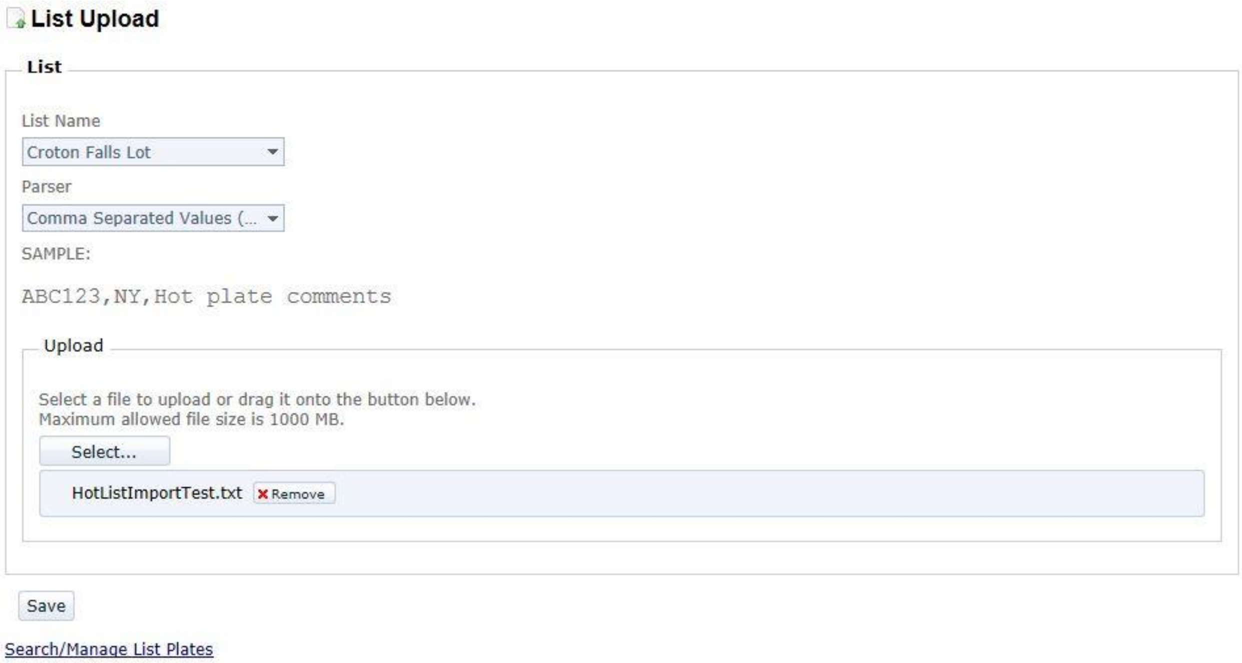


Select a file to upload or drag it onto the button below.
Maximum allowed file size is 1000 MB.

Figure 99 — List Upload Screen

(2) Select the List to update from the **List Name** drop-down and the parser that will interpret the data in the file to be uploaded. You will only see lists to which you have rights.

NOTE: Below the **Parser** drop down menu, you will see a sample of the selected parser's format.



List Upload

List

List Name: Croton Falls Lot

Parser: Comma Separated Values (...

SAMPLE:

```
ABC123,NY,Hot plate comments
```

Upload

Select a file to upload or drag it onto the button below.
Maximum allowed file size is 1000 MB.

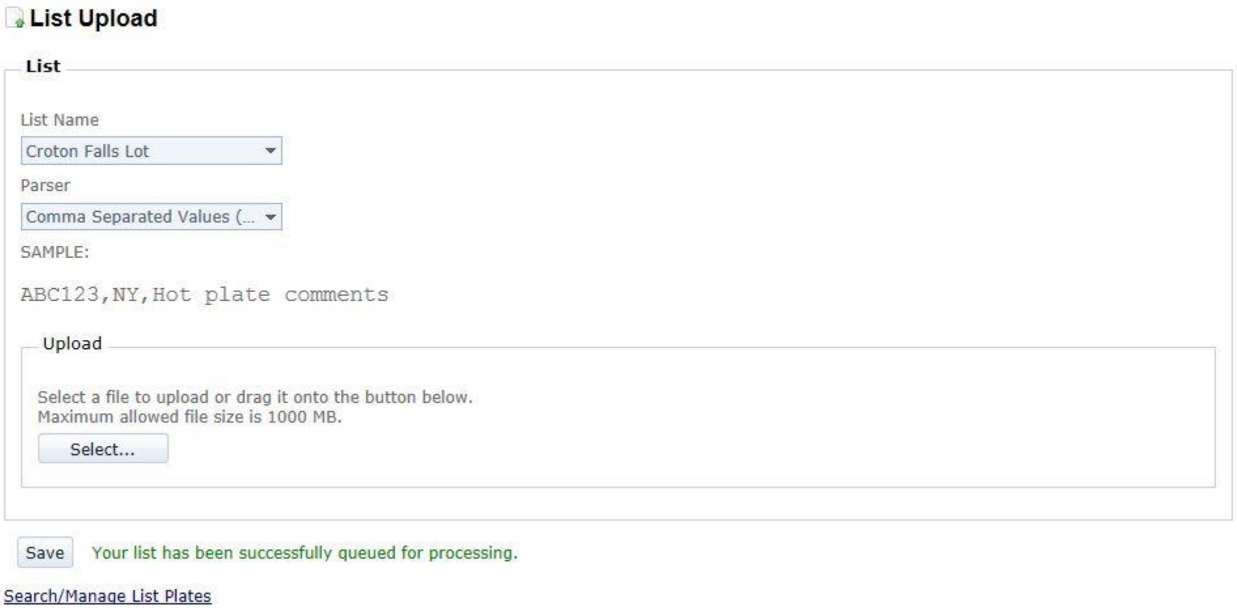
Figure 100 — List Upload Screen (List and Parser Selected)

(3) Press the **Select** button and browse to the location of the file to be uploaded.

NOTE: The file must be smaller than 1000 MB.

(4) Press **Save**. You will see the screen shown below in Figure 101.

NOTE: Your list will be updated when the EOC next processes updates.



List Upload

List

List Name

Croton Falls Lot

Parser

Comma Separated Values (...

SAMPLE:

```
ABC123,NY,Hot plate comments
```

Upload

Select a file to upload or drag it onto the button below.
Maximum allowed file size is 1000 MB.

Your list has been successfully queued for processing.

Figure 101 — List Upload Screen (List Queued)

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Chapter 7 — System Configuration

Introduction

The **System** tab of the EOC allows you to:

- Set up and manage the organization of your EOC implementation (**Device Manager**),
- Define and schedule system maintenance tasks (**System Tasks**),
- Audit activities within your EOC implementation (**Log Messages** or **Audit Messages**), and
- Modify EOC Application settings (**App Settings**).

Device Manager

The Device Manager area of the System Configuration tab allows you to set up your local organizations inside EOC, including such elements as:

- Geographical areas
- Organizational groupings
- Vehicles
- Mobile Cameras
- Fixed Cameras, and
- FCUs (Field Control Units).

It is a useful exercise to plot out your site configuration before you start to build it in EOC, although it is simple to reorganize within the EOC. We have included a simple tutorial on how to set up a system below.

Device Manager also allows you to move cameras and other elements easily within EOC, as well enable and disable individual elements.

Types of Nodes

Device Manager allows for four different types of elements or **nodes**:

- Car — A container for mobile cameras
- FCU (Field Control Unit) — A container for fixed cameras
- Folder — Geographical areas and/or organizational groups, and
- Server — Remote Server.

❑ Sample Hierarchy

A hierarchical diagram of a typical EOC system shows how the different types of nodes relate.

Consider this scenario: You have three towns in your county, each of which has one car with two cameras installed and two fixed cameras at various locations in each town. Your system hierarchy (with the type of node in parentheses) would look like this.

> **NOTE:** Nodes of the same type below the parent level should be given unique names within their domain when you create them. For example, refer to Figure 102 below.

- **County** (domain, but also a folder)
    - **Town 1** (folder)
        - Car T11 (car)
            - Camera T11 (mobile camera)
            - Camera T12 (mobile camera)
        - FCU T11 (FCU)
            - Pole Camera T11 (fixed camera)
            - Pole Camera T12 (fixed camera)
    - **Town 2** (folder)
        - Car T21 (car)
            - Camera T21 (mobile camera)
            - Camera T22 (mobile camera)
        - FCU T21 (FCU)
            - Pole Camera T21 (fixed camera)
            - Pole Camera T22 (fixed camera)
    - **Town 3** (folder)
        - Car T31 (car)
            - Camera T31 (mobile camera)
            - Camera T32 (mobile camera)
        - **FCU T31** (FCU)
            - Pole Camera T31 (fixed camera)
            - Pole Camera T32 (fixed camera)

Figure 102 — Sample EOC System Hierarchy

Prerequisites

Before creating the system configuration for your EOC implementation, you must create the domains for it. A domain is how the EOC collects data and sets the permissions for access to it.

The EOC is installed with a default domain, as well as a default user and group.

Creating a Domain

An EOC domain provides a mechanism to collect a specified data set and control permissions to the access for that data. For example, you could use a separate domain inside the EOC to collect data from a list that you wanted to have restricted access.

In the **Device Manager**, you will not see the **Create Domain** function unless you have permissions to create a domain.

NOTE: You cannot delete a domain once you have created it.

To create a domain, perform the following steps:

(1) Press the **Create Domain** button and the screen shown in Figure 103 will appear.

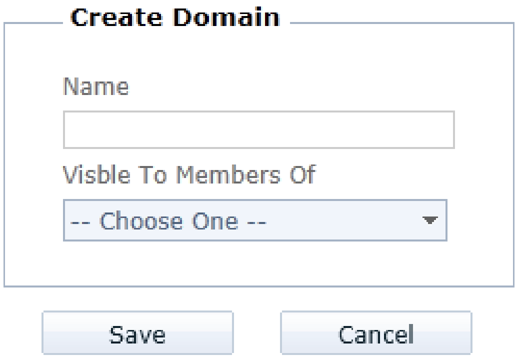
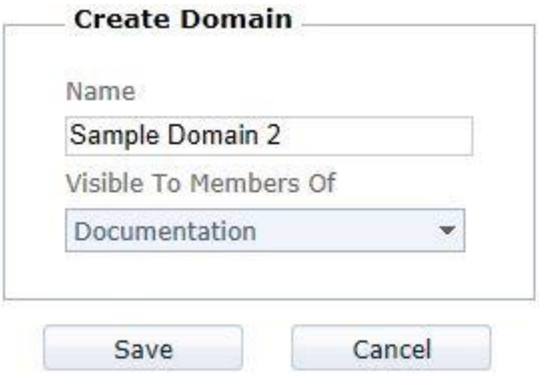


Figure 103 — Create Domain Initial Screen

(2) Select a group for the domain to be visible to the members of. You must be a member of this group to select the group.

NOTE: The “Visible To Members Of” list is limited to what you can see with your user profile.



Name: Sample Domain 2

Visible To Members Of: Documentation

Figure 104 — Create Domain Example

(3) If you are a member of the group you select, the domain will be created and appear in the list of domains and nodes in the left hand side of the display (see Figure 105).

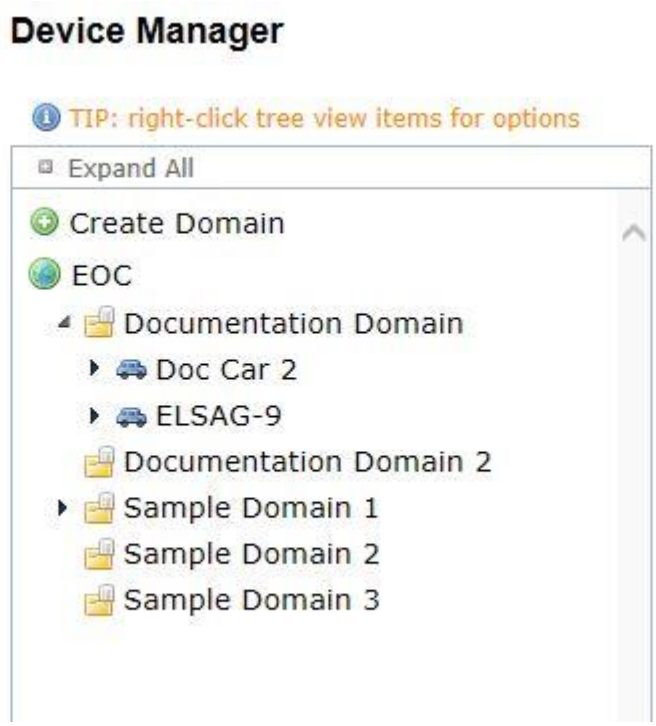


Figure 105 — List of Domains with New Domain

Now you can select the new domain and create the nodes that will define its organization.

Navigating the Device Manager Interface

Navigating the interface on the Device Manager page is simple. In the left hand pane, right click to see the command options (also see Figure 106):

- Details
- Create
- Edit
- Delete
- Export, and
- Close.

Adding a Node

Each of the top-level nodes in your EOC implementation represents a domain that you have created in the EOC database. Your EOC installation comes with one default domain set up – one of the domains is named **Administrative**.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Adding a Node or Branch

A node is a single item in a tree; a branch is part of a domain with nodes below it. You can delete a single node or an entire branch at once. You access the editing options for nodes in the Device Manager area by right clicking on an existing node. When you right-click, you will see the menu shown below in Figure 106. Then perform the steps that follow.

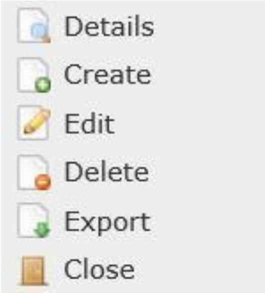


Figure 106 — Device Manager Edit Menu

(1) To add a node, select the existing node that you want for the parent of the new node. For example, say you wanted to create a folder under **Sample Domain 2** named **West Side**.

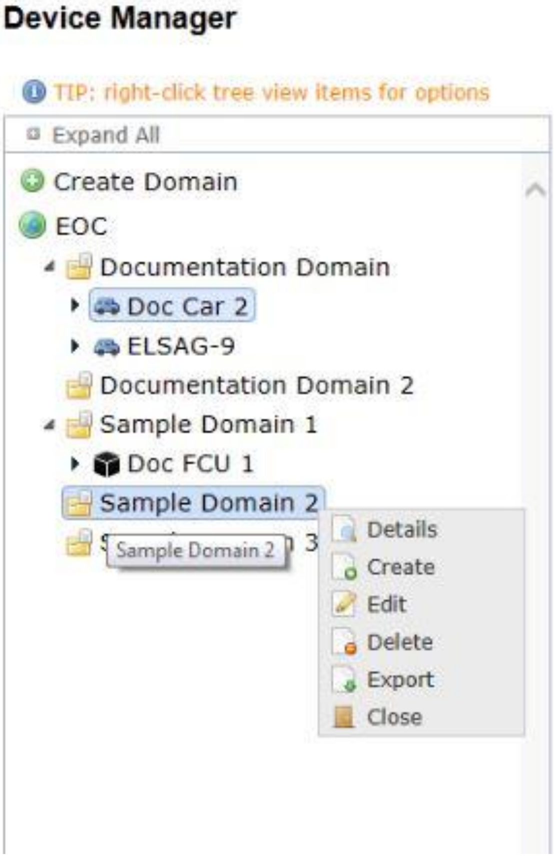
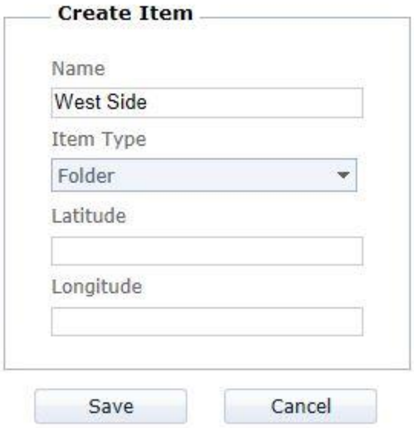


Figure 107 — Device Manager Initial Screen

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(2) First, right-click on the **Sample Domain 2** node and select **Create**. You will see the Create Item dialog prompt as shown in Figure 108 that follows.



Name: West Side

Item Type: Folder

Figure 108 — Create Item Dialog

(3) Type **West Side** in the **Name** box and select **Folder** from the **Item Type** drop-down.

(4) **Latitude** and **Longitude** are option entries. Best use is for fixed cameras which never move. The Latitude and Longitude can be set one time on the EOC.

(5) Press **Save**. Your newly created node appears where you created it as shown in Figure 109.

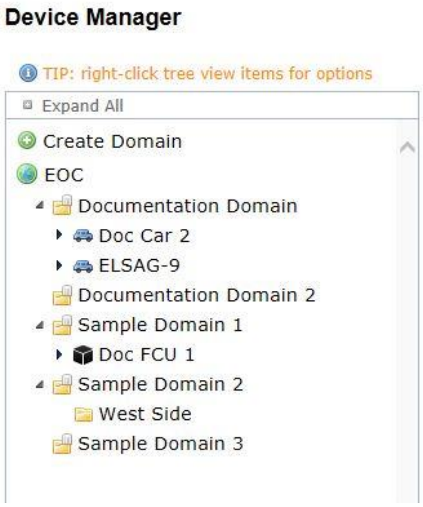


Figure 109 — Folder Created

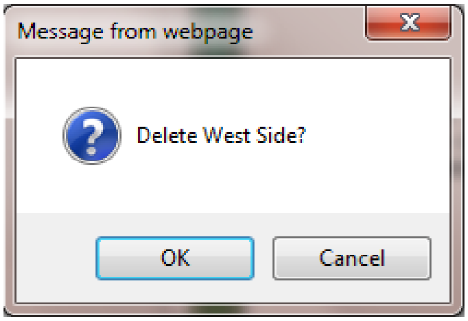
Deleting a Node or Branch

A node is a single item in a tree; a branch is part of a domain with nodes below it. You can delete a single node or an entire branch at once.

Deleting a node or branch does not completely delete it from the database, since that would make all the associated historical data useless. Instead, the EOC makes the node or branch invisible when it is deleted.

(1) To delete, right-click on the node or branch you want to delete. (In this example, we are deleting the node we just created under **Sample Domain 2**.)

(2) Select **Delete**. You see the following warning message screen shown in Figure 110.



Delete West Side?

Figure 110 — Delete Node Warning Message

(3) Press **OK** to delete the node. Referring to Figure 111 that follows, the deleted node is no longer visible.

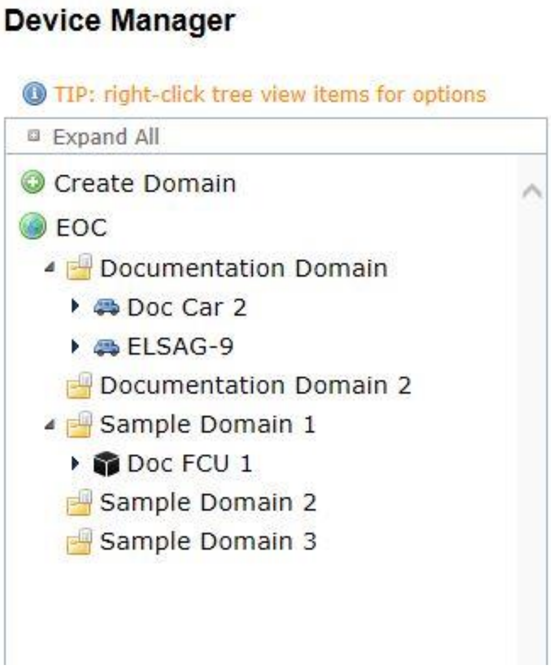
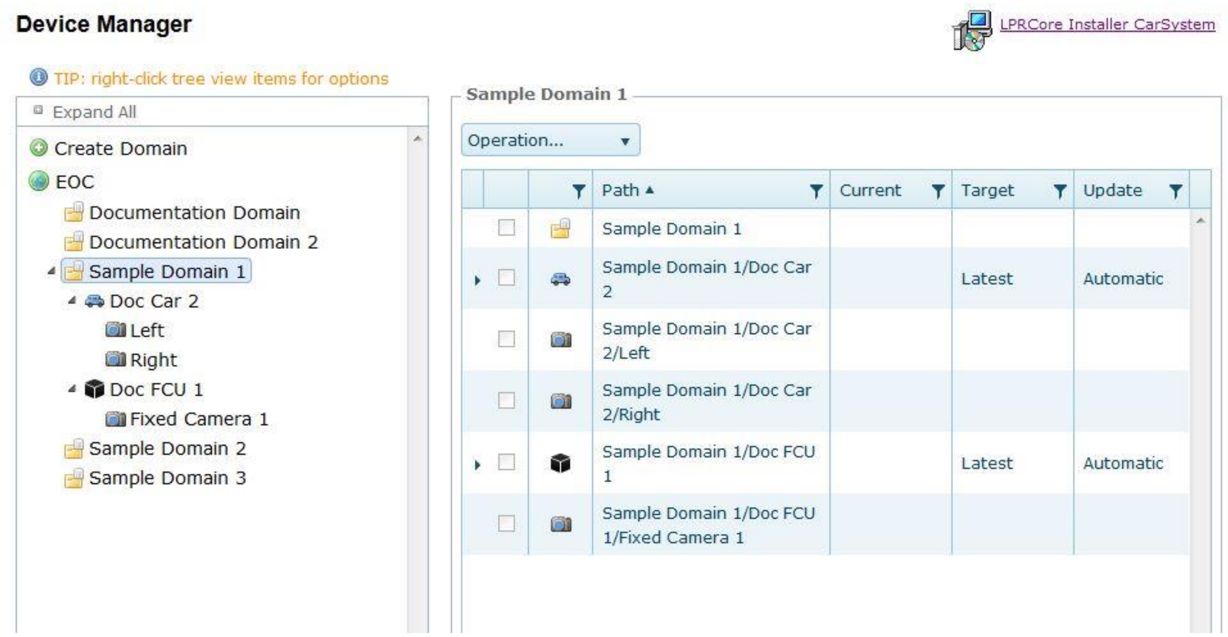


Figure 111 — Node Deleted

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Viewing a Node

To view information about a node click on a node name. You will see a display as shown in Figure 112.



Device Manager

LPRCore Installer CarSystem

TIP: right-click tree view items for options

Expand All

- Create Domain
- EOC
  - Documentation Domain
  - Documentation Domain 2
  - Sample Domain 1
    - Doc Car 2
      - Left
      - Right
    - Doc FCU 1
      - Fixed Camera 1
  - Sample Domain 2
  - Sample Domain 3

Sample Domain 1

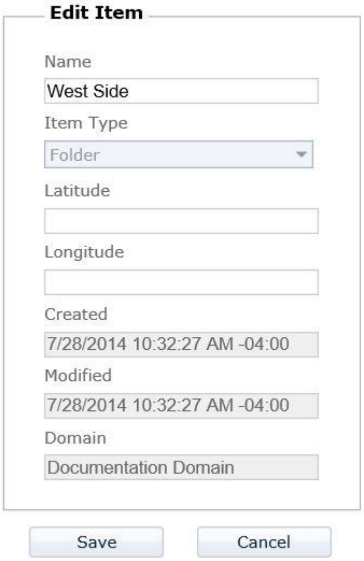
Operation... ▾

			Path ▲	Current	Target	Update
	□		Sample Domain 1			
▸	□		Sample Domain 1/Doc Car 2		Latest	Automatic
	□		Sample Domain 1/Doc Car 2/Left			
	□		Sample Domain 1/Doc Car 2/Right			
▸	□		Sample Domain 1/Doc FCU 1		Latest	Automatic
	□		Sample Domain 1/Doc FCU 1/Fixed Camera 1			

Figure 112 — View Node

Editing Node Information

To edit a node’s information, right click on the node and select **Edit**. You will see the display shown in Figure 113. Change the information you want to change, and then press **Save**.



Edit Item

Name: West Side

Item Type: Folder

Latitude:

Longitude:

Created: 7/28/2014 10:32:27 AM -04:00

Modified: 7/28/2014 10:32:27 AM -04:00

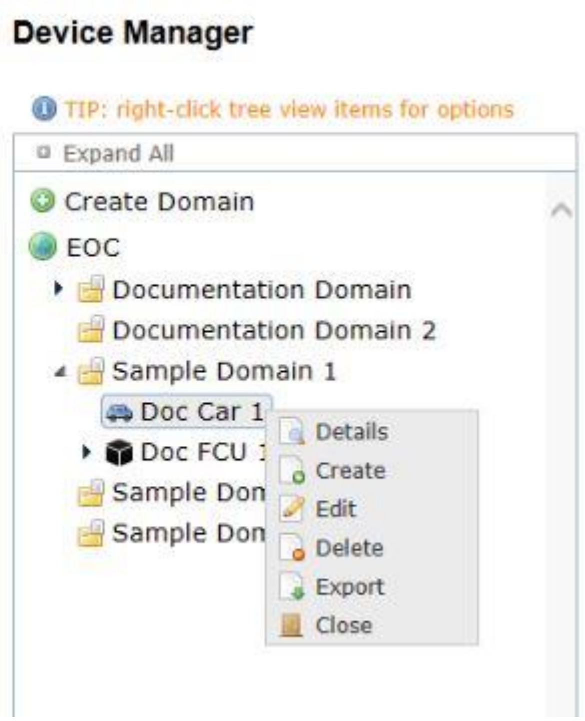
Domain: Documentation Domain

Figure 113 — Edit Node

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Adding a Camera

Adding a camera to a car or FCU node allows the EOC administrator to give a friendly name to the camera. By default, camera names come automatically from information on the camera. For example, **Doc Car 1** has two cameras and you want to label them “Left” and “Right.” Referring to Figure 114, right click on **Doc Car 1** and select **Create**.



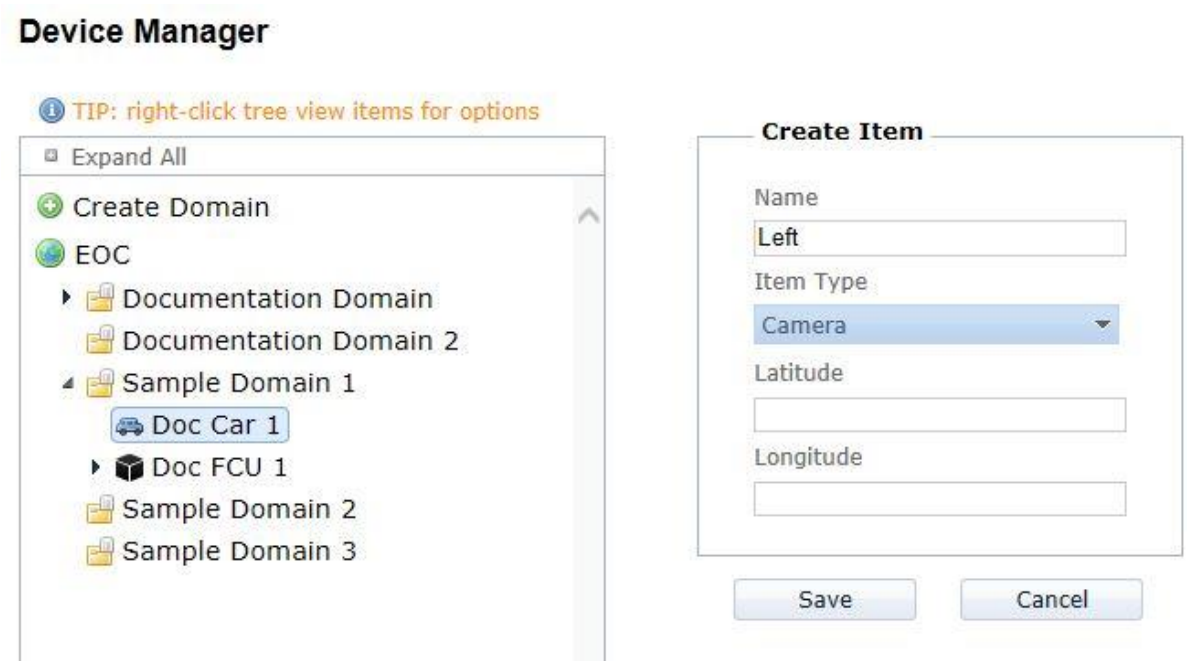
Device Manager

TIP: right-click tree view items for options

Figure 114 — Adding a Camera

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

As shown in Figure 115, enter the Name “Left” and select **Item Type Camera** (there is only one Item Type when a Car or FCU node is being modified). Repeat these steps to create the Right camera.

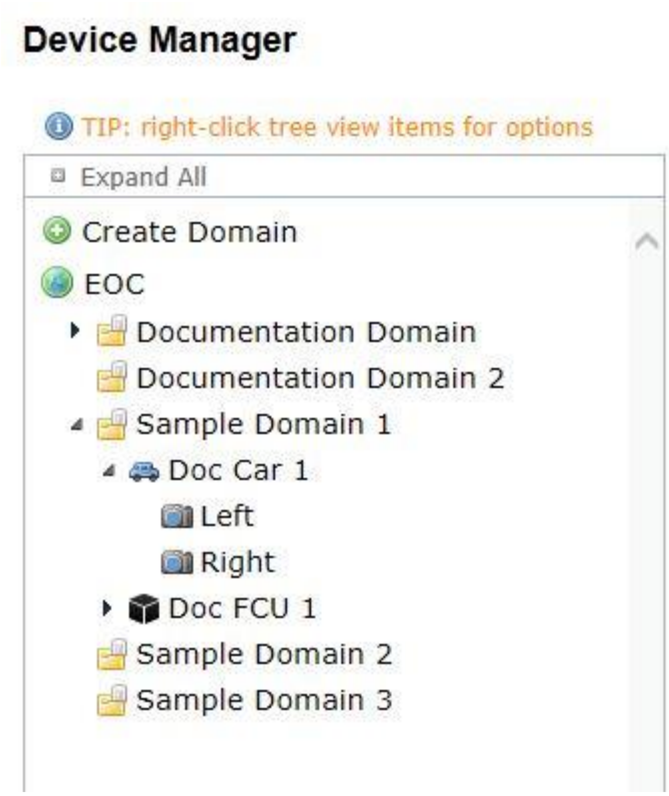


Name: Left

Item Type: Camera

Figure 115 — Create Item Type Camera

As shown in Figure 116, cameras are listed under Doc Car 1 with friendly names.



Device Manager

TIP: right-click tree view items for options

Expand All

Create Domain

- EOC
  - Documentation Domain
  - Documentation Domain 2
  - Sample Domain 1
    - Doc Car 1
      - Left
      - Right
    - Doc FCU 1
  - Sample Domain 2
  - Sample Domain 3

Figure 116 — Friendly-named Cameras

NOTE: If the camera is being added to an FCU (fixed location that doesn't move) you can enter the Latitude and Longitude coordinates for that FCU so that FCU would not require a GPS.

Exporting Node Information to CarSystem

The **Export** command allows you to export system configuration information to a thumb drive or external storage device so that when you install your CarSystem implementation it will communicate correctly with the EOC.

You should perform this step before you install CarSystem, since the configuration information exported from EOC is necessary to install and configure CarSystem correctly. The output of the export process is an XML file that the CarSystem installation process can then read. The user can export in two ways, by exporting a single node and by exporting multiple nodes at one time

❑ Export a Single Node

To export a single node use the following steps:

(1) Right-click on the node and select **Export**. You will see the following display shown in Figure 117. The screen shown in Figure 118 is as it would appear if you are using Microsoft Internet Explorer, in which case the user would select **Save**.

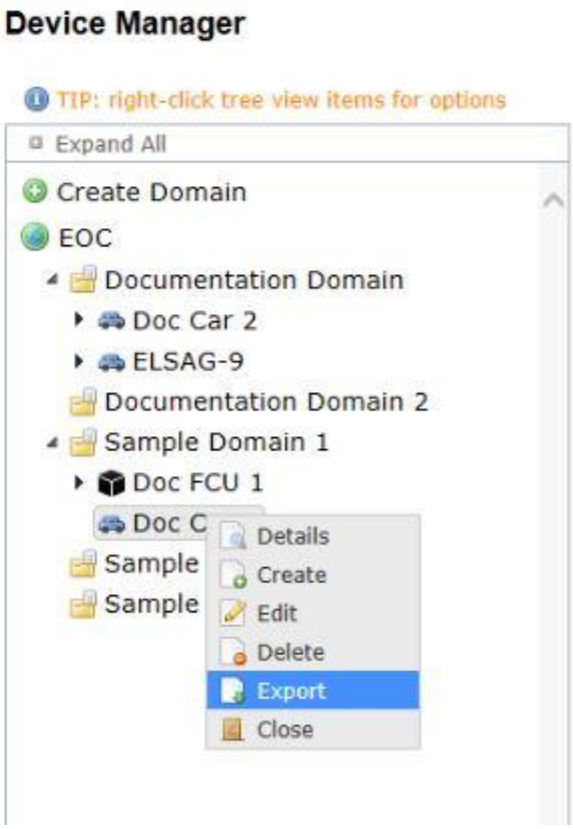
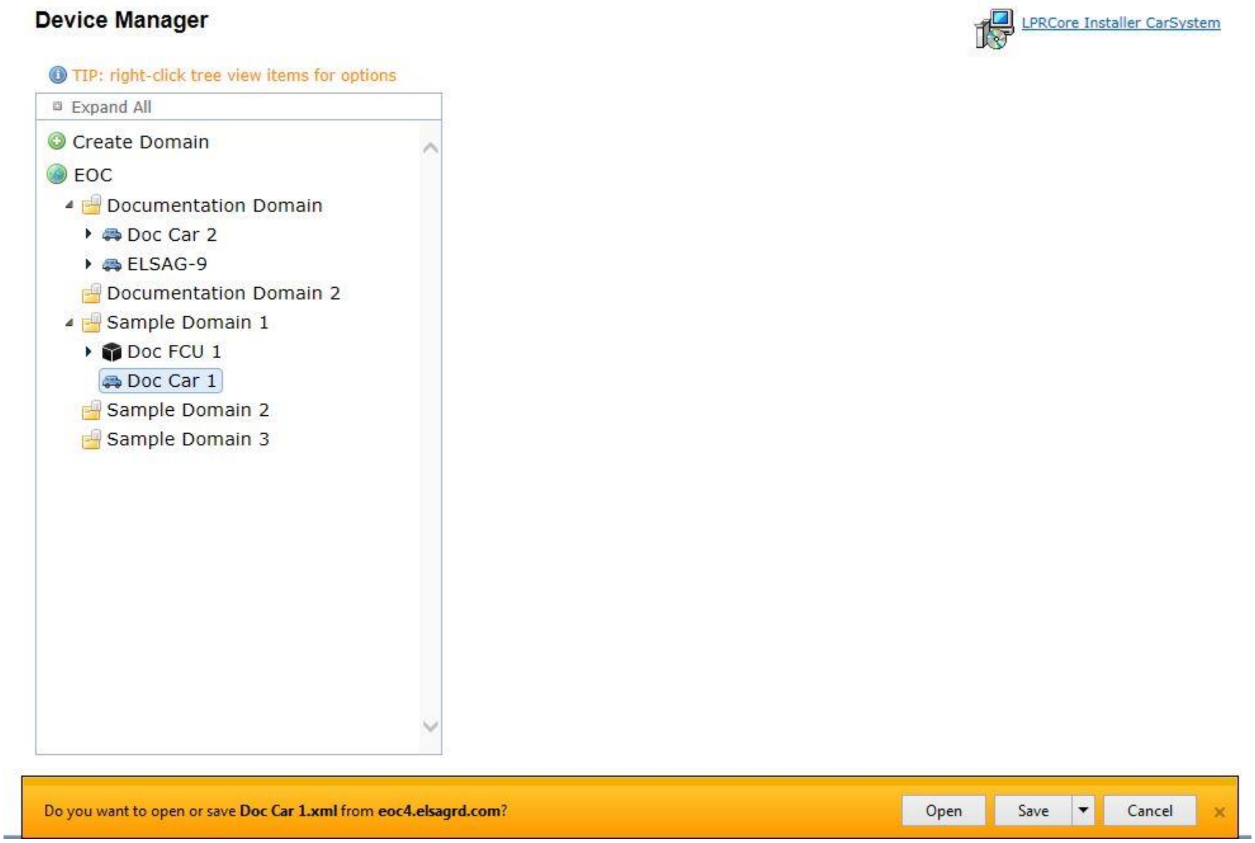


Figure 117 — Export Node Menu



Do you want to open or save **Doc Car 1.xml** from **eoc4.elsagrd.com**?

Figure 118 — Open or Save Node XML File

(3) Select Save and the file will be saved to your Downloads folder (in Windows 7).

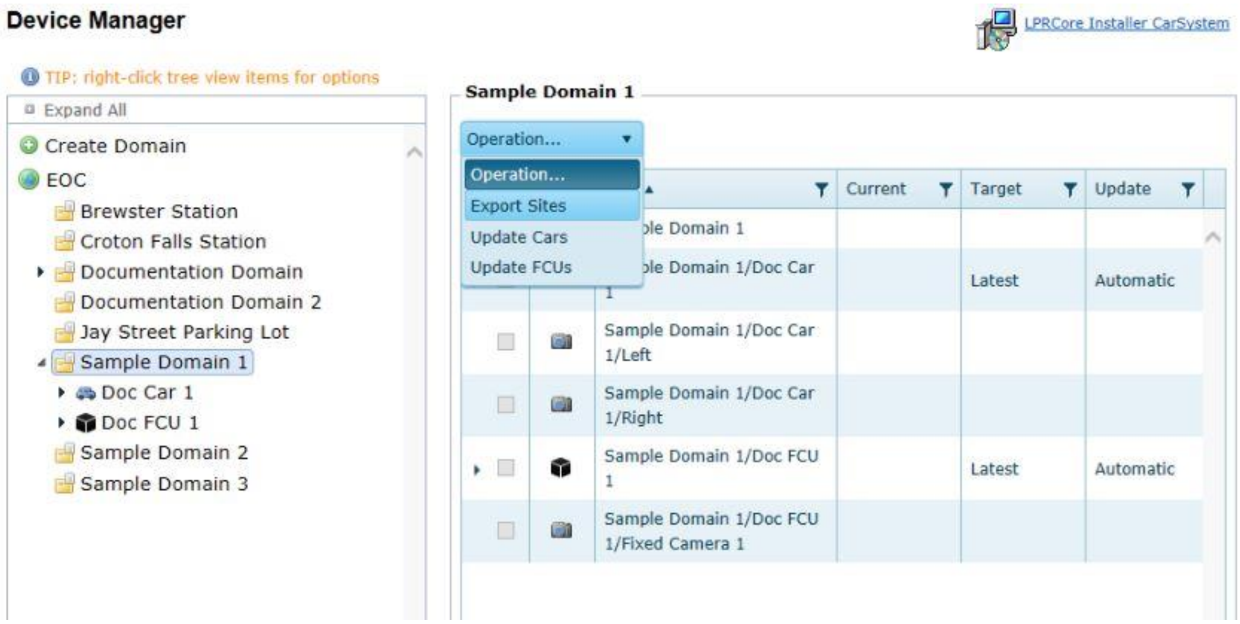
(4) Copy the XML file to your USB stick for use in the CarSystem install.

❑ Exporting Multiple Nodes at One Time

If you have created multiple cars or FCUs that will be installed all at once, you can export the XML files at the same time.

Referring to Figure 119, you want to export Sample Domain 1 Doc Car 1 and Doc FCU 1 at the same time. Click on node Sample Domain 1 to reveal the node details.

Click on the Operations drop down and select Export Sites. The sites to be exported are automatically checked off. You can modify the selections manually. Once your selections are correct, click the Export button. A zipped file containing the XML files will be downloaded to your local PC.



			Current	Target	Update
		ple Domain 1			
		ple Domain 1/Doc Car 1		Latest	Automatic
□		Sample Domain 1/Doc Car 1/Left			
□		Sample Domain 1/Doc Car 1/Right			
□		Sample Domain 1/Doc FCU 1		Latest	Automatic
□		Sample Domain 1/Doc FCU 1/Fixed Camera 1			

Figure 119 — Exporting Multiple Nodes at One Time

Moving Cars or Cameras from One Site to Another

You can move nodes from one place to another in your EOC system configuration simply by dragging the node you want to move and dropping it in its new location. The system will inform you if the move violates any system rules and will keep you from doing it if it will cause access difficulties.

❑ Implications for Data

When you move nodes from one place to another within the EOC system configuration, you should be aware of the following potential effects of the move on the quality and integrity of the data stored in the database.

> **NOTE:** Deleting a node does not remove it from the database; it simply makes it invisible to the UI. This is so that you can continue to search on and generate reports on historical data associated with that node.

Upgrading Car and FCU CarSystem Software

When the EOC is upgraded to a new version it is advisable to upgrade all cars and mobile units to the latest version as soon as possible. There are two ways to upgrade remote devices: manually and automatically from the EOC.

> **NOTE:** Earlier version of CarSystem Mobile and CarSystem Fixed (6.6 and lower) will not auto-upgrade and have to be upgraded manually.

❑ Manual Upgrades

Manual upgrades require someone to physically move a copy of the LPRCore Installer CarSystem.msi installer file from the EOC to the remote site and run the installer on that device. This could be by remote access or physically visiting the remote site.
To access the LPRCore Installer CarSystem.msi installer file, perform the following steps:

(1) Log into the EOC.

(2) Select **System > Device Manager**.

(3) Referring to Figure 120, on the Device Manager page click the LPRCore Installer CarSystem link.

LPRCore Installer CarSystem

Figure 120 — LPRCore Installer CarSystem Link

(4) You will be asked where you want to save the file. Select a location and click Save.

If the remote site has remote access, perform the following steps:

(1) Connect to the remote site.

(2) Copy LPRCore Installer CarSystem.msi installer to the site's PC.

(3) Run the installer on the remote site.

If the remote site does not have internet access to the EOC, perform the following steps:

(1) Follow the above steps from a computer that has access to the EOC and save the installer to a thumbdrive you can bring to the remote site.

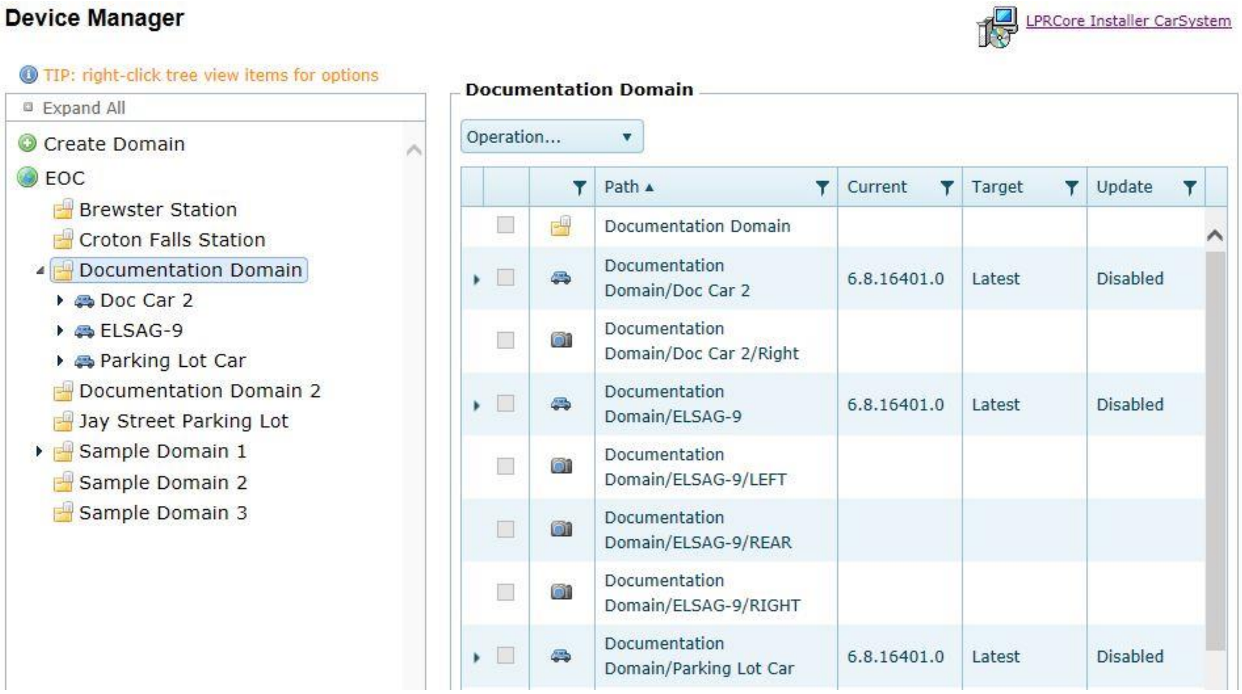
(2) At the remote site run the installer and upgrade the existing CarSystem software.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

❑ Automatic Upgrading from an EOC

EOC 5.1 and later Device Manager allows the automatic upgrading from the EOC of a remote site (car or FCU) as long as the remote site has a wired or wireless connection to the EOC. Follow these steps to initiate the remote site upgrades:

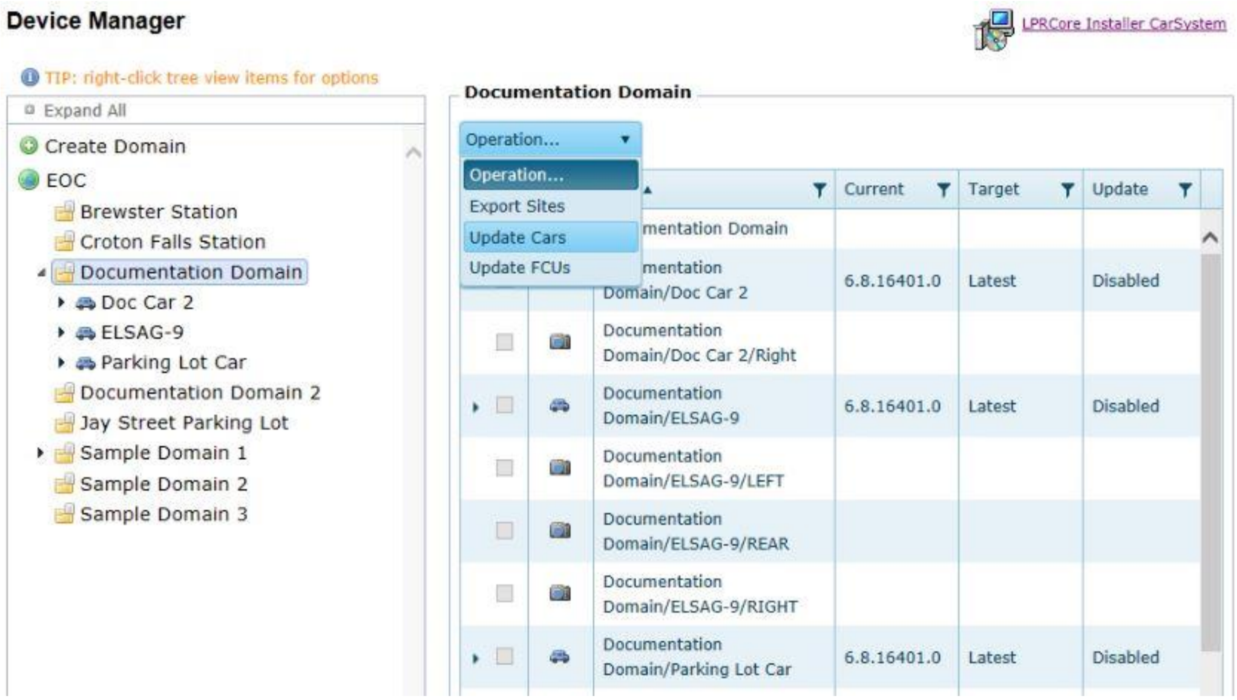
(1) You can select one or multiple sites to upgrade at the same time. Referring to Figure 121, to upgrade one remote site select that single car or FCU in the left panel. If upgrading multiple cars or FCUs select the top of the node you want to upgrade. In the below example all sites under node **Documentation Domain** will be displayed on the node detail view.



		Path ▲	Current	Target	Update
	☐	Documentation Domain			
▸	☐	Documentation Domain/Doc Car 2	6.8.16401.0	Latest	Disabled
	☐	Documentation Domain/Doc Car 2/Right			
▸	☐	Documentation Domain/ELSAG-9	6.8.16401.0	Latest	Disabled
	☐	Documentation Domain/ELSAG-9/LEFT			
	☐	Documentation Domain/ELSAG-9/REAR			
	☐	Documentation Domain/ELSAG-9/RIGHT			
▸	☐	Documentation Domain/Parking Lot Car	6.8.16401.0	Latest	Disabled

Figure 121 — Documentation Domain Example

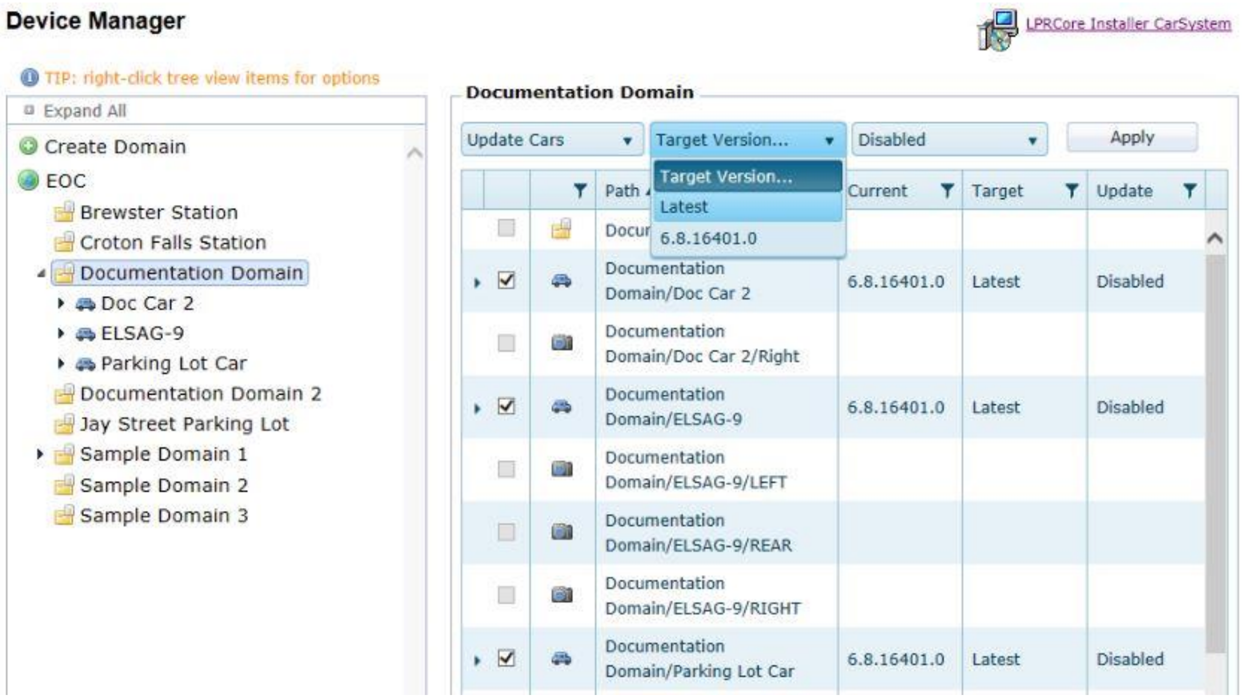
(2) Referring to Figure 122, select the **Operation** dropdown and then either **Update Cars** or **Update FCUs**. The sites to be upgraded will automatically be checked as shown in Figure 122.



			Current	Target	Update
		mentation Domain			
		mentation Domain/Doc Car 2	6.8.16401.0	Latest	Disabled
	□	Documentation Domain/Doc Car 2/Right			
	□	Documentation Domain/ELSAG-9	6.8.16401.0	Latest	Disabled
	□	Documentation Domain/ELSAG-9/LEFT			
	□	Documentation Domain/ELSAG-9/REAR			
	□	Documentation Domain/ELSAG-9/RIGHT			
	□	Documentation Domain/Parking Lot Car	6.8.16401.0	Latest	Disabled

Figure 122 — Operation Dropdown

(3) Referring to Figure 123, select the **Target Version** dropdown and select **Latest Version**.



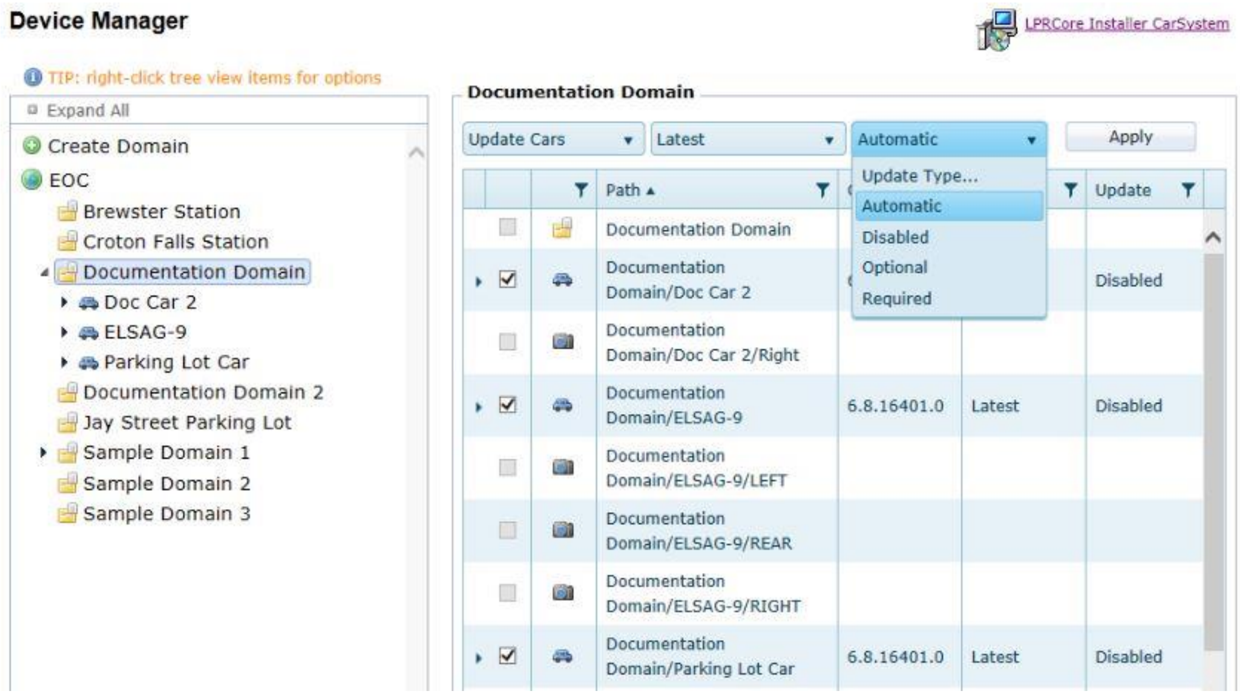
- EOC
  - Brewster Station
  - Croton Falls Station
  - Documentation Domain
    - Doc Car 2
    - ELSAG-9
    - Parking Lot Car
  - Documentation Domain 2
  - Jay Street Parking Lot
  - Sample Domain 1
  - Sample Domain 2
  - Sample Domain 3

Documentation Domain

	Path	Current	Target	Update
□	Docur			
☑	Documentation Domain/Doc Car 2	6.8.16401.0	Latest	Disabled
□	Documentation Domain/Doc Car 2/Right			
☑	Documentation Domain/ELSAG-9	6.8.16401.0	Latest	Disabled
□	Documentation Domain/ELSAG-9/LEFT			
□	Documentation Domain/ELSAG-9/REAR			
□	Documentation Domain/ELSAG-9/RIGHT			
☑	Documentation Domain/Parking Lot Car	6.8.16401.0	Latest	Disabled

Figure 123 — Target Version to Latest Version

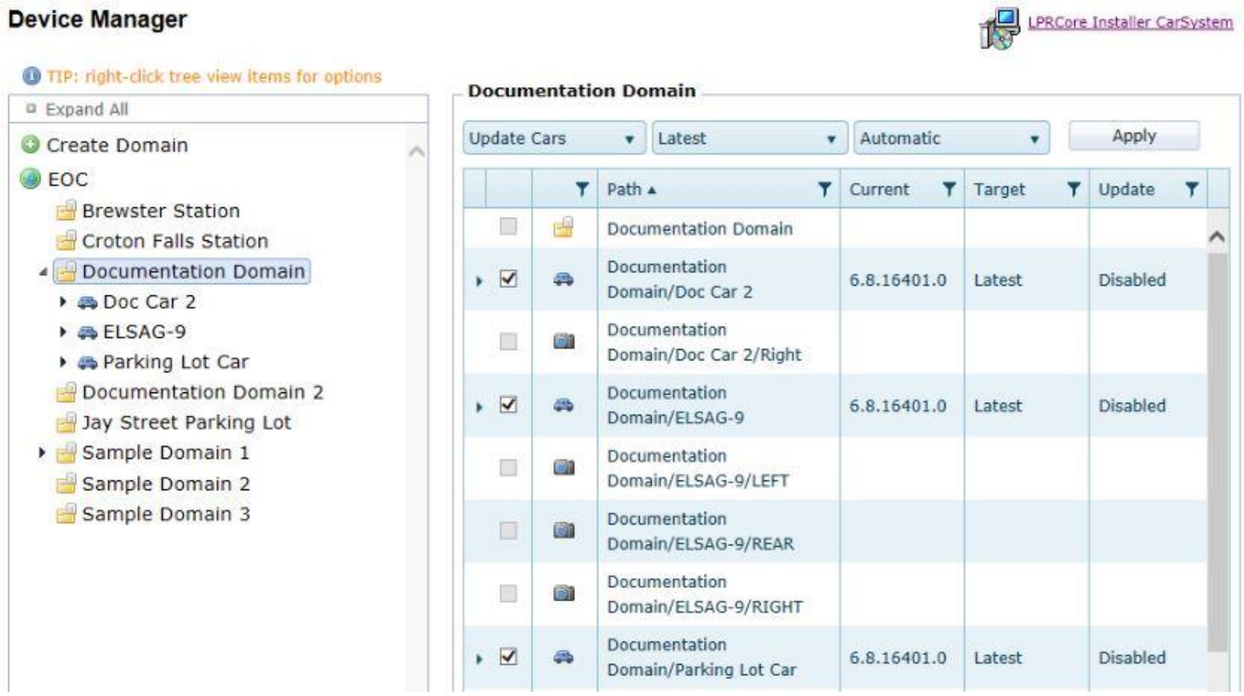
(4) Referring to Figure 124, select the **Update Type** dropdown and select **Automatic**.



			Path ▲			Update
	☐		Documentation Domain			
▸	☑		Documentation Domain/Doc Car 2			Disabled
	☐		Documentation Domain/Doc Car 2/Right			
▸	☑		Documentation Domain/ELSAG-9	6.8.16401.0	Latest	Disabled
	☐		Documentation Domain/ELSAG-9/LEFT			
	☐		Documentation Domain/ELSAG-9/REAR			
	☐		Documentation Domain/ELSAG-9/RIGHT			
▸	☑		Documentation Domain/Parking Lot Car	6.8.16401.0	Latest	Disabled

Figure 124 — Update Type to Automatic

(5) Referring to Figure 125, if all options are correct, click **Apply**.



Device Manager

LPRCore Installer CarSystem

TIP: right-click tree view items for options

Expand All

- Create Domain
- EOC
  - Brewster Station
  - Croton Falls Station
  - Documentation Domain
    - Doc Car 2
    - ELSAG-9
    - Parking Lot Car
  - Documentation Domain 2
  - Jay Street Parking Lot
  - Sample Domain 1
  - Sample Domain 2
  - Sample Domain 3

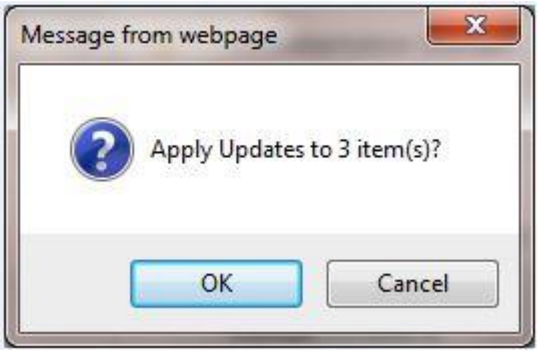
Documentation Domain

Update Cars ▾ | Latest ▾ | Automatic ▾ | Apply

			Path ▴	Current	Target	Update
	□		Documentation Domain			
▸	☑		Documentation Domain/Doc Car 2	6.8.16401.0	Latest	Disabled
	□		Documentation Domain/Doc Car 2/Right			
▸	☑		Documentation Domain/ELSAG-9	6.8.16401.0	Latest	Disabled
	□		Documentation Domain/ELSAG-9/LEFT			
	□		Documentation Domain/ELSAG-9/REAR			
	□		Documentation Domain/ELSAG-9/RIGHT			
▸	☑		Documentation Domain/Parking Lot Car	6.8.16401.0	Latest	Disabled

Figure 125 — Review Documentation Domain Settings

(6) Referring to Figure 126, you will be asked to confirm the number of remote sites that will upgrade.



Message from webpage

Apply Updates to 3 item(s)?

OK Cancel

Figure 126 — Apply Updates Confirmation

At this point the EOC will start transmitting the LPRCore Installer CarSystem.msi installer to the remote site. Network bandwidth from the EOC and at the remote site determines how long it will take for the sites to finish the upgrade. When the sites are upgraded Device Manager will display the version number in the **Current** column.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

- ❑ **Considerations**

It is best that the remote site knows an upgrade is being pushed down to them. If a CarSystem is running at upgrade time, CarSystem process will be killed so that the upgrade will proceed. That might interrupt a deployed patrol car.

Time the upgrade for off-peak hours if down time or Internet bandwidth is a concern.

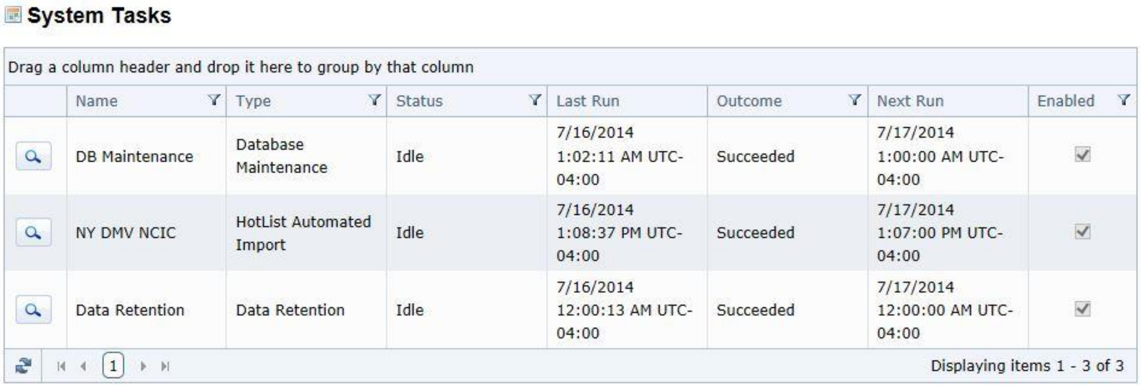
Outgoing network bandwidth speed might be affected if upgrading many remote sites at one time.

System Tasks

The **System Tasks** selection allows you to view the available system management tasks, schedule them and run them. Running these ensures better EOC system and database performance, so you should either schedule them to run automatically or be sure to run them on a regular basis.

All new EOC installations have default tasks for Database Maintenance and Data Retention, which should be scheduled to run daily. Midnight is the default time. Also, note that if you do not have permissions to see the tasks, you will not see them. Refer to Figure 127 and the steps that follow:

(1) Select **System** > **System Tasks**. You will see this screen, which shows the characteristics of each of the system tasks available to you.



System Tasks

Drag a column header and drop it here to group by that column

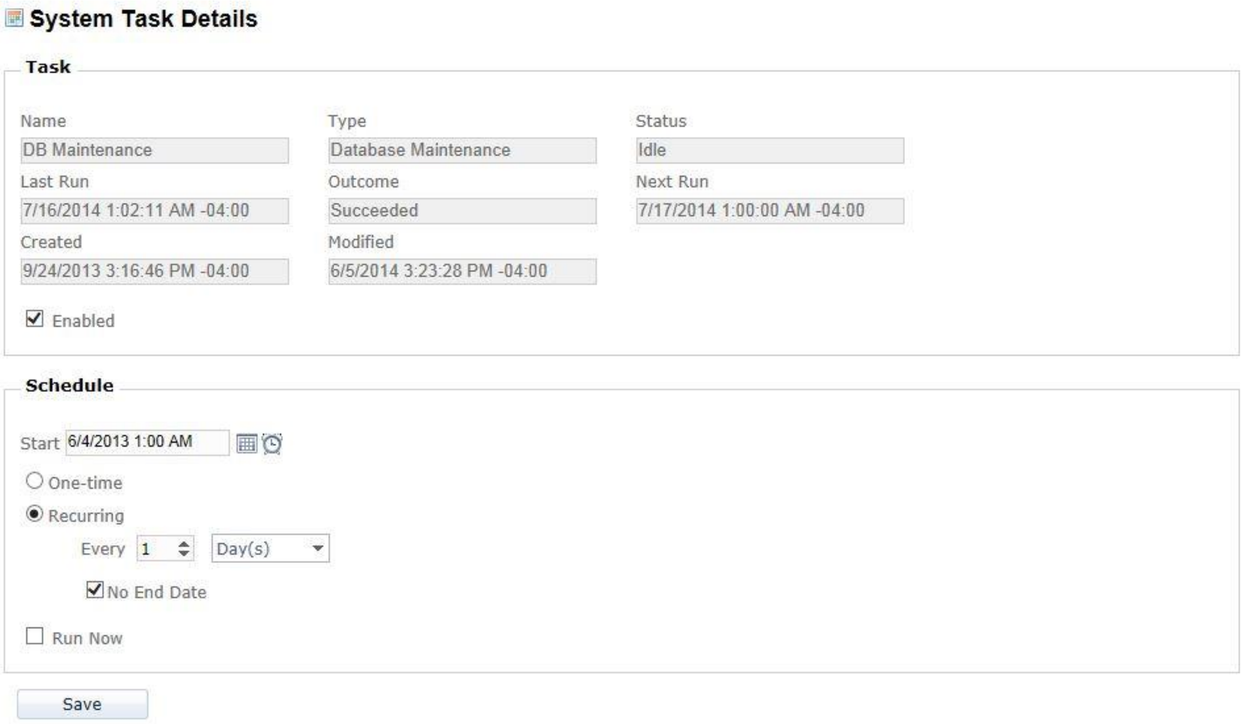
	Name	Type	Status	Last Run	Outcome	Next Run	Enabled
🔍	DB Maintenance	Database Maintenance	Idle	7/16/2014 1:02:11 AM UTC-04:00	Succeeded	7/17/2014 1:00:00 AM UTC-04:00	☑
🔍	NY DMV NCIC	HotList Automated Import	Idle	7/16/2014 1:08:37 PM UTC-04:00	Succeeded	7/17/2014 1:07:00 PM UTC-04:00	☑
🔍	Data Retention	Data Retention	Idle	7/16/2014 12:00:13 AM UTC-04:00	Succeeded	7/17/2014 12:00:00 AM UTC-04:00	☑

Displaying items 1 - 3 of 3

Figure 127 — System Tasks List

If you have automated a List Import you will also see it listed here. As shown in Figure 127, NY DMV NCIC is automated to be imported daily at 1:07 PM.

(2) Select **Details** (magnifying glass icon) to view or edit the details of the task, including its schedule. See Figure 128.



System Task Details

Task

Name	Type	Status
DB Maintenance	Database Maintenance	Idle

Last Run	Outcome	Next Run
7/16/2014 1:02:11 AM -04:00	Succeeded	7/17/2014 1:00:00 AM -04:00

Created	Modified
9/24/2013 3:16:46 PM -04:00	6/5/2014 3:23:28 PM -04:00

☑ Enabled

Schedule

Start 6/4/2013 1:00 AM

○ One-time

● Recurring

Every 1 Day(s)

☑ No End Date

□ Run Now

Figure 128 — System Tasks Details

(3) If you have the appropriate permissions, you can change the schedule or other characteristics of the task, including **Start** time, whether the task should be run **One-time** or on a **Recurring** basis, and the day and time a recurring task should run.

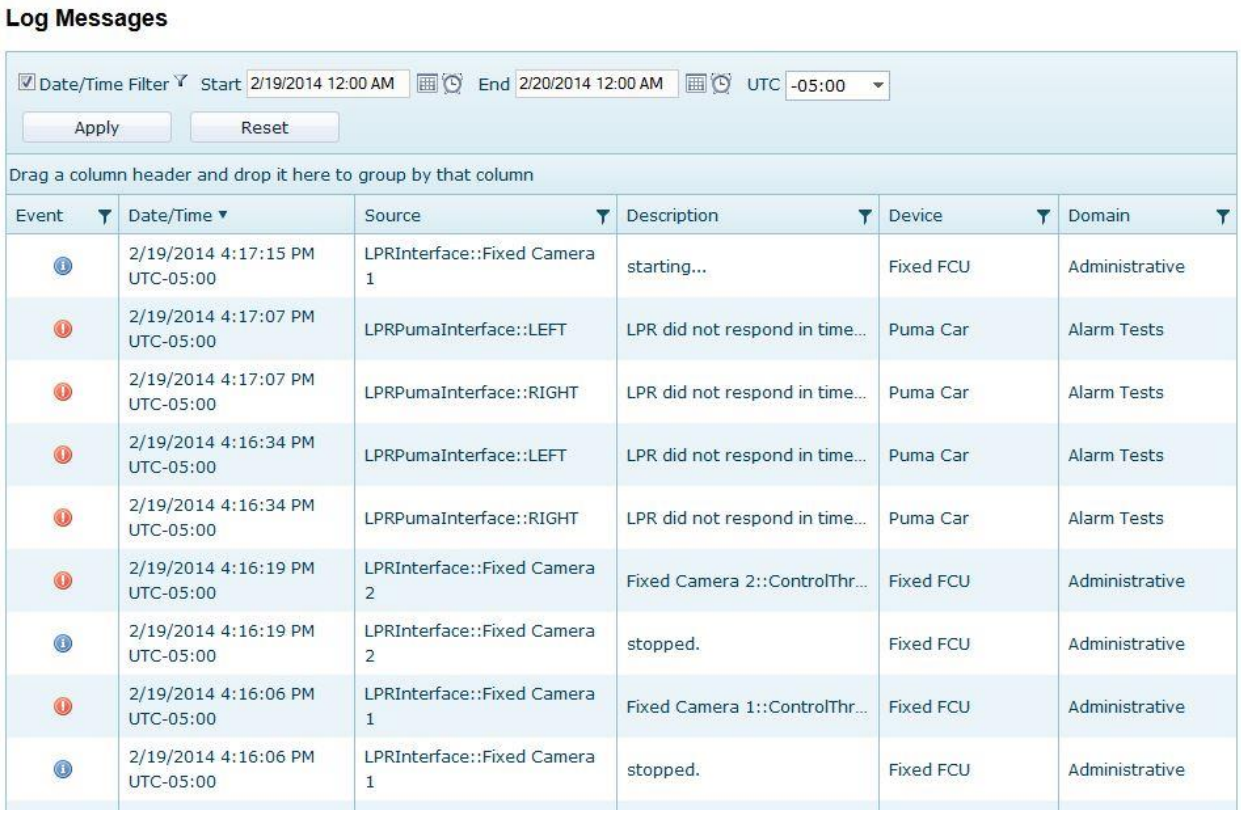
NOTE: To alter the date, click on the calendar icon and select the date to run the task; to change the time, click on the clock icon and set a time.

(4) Press **Save** to save any changes.

Log Messages

The Log Messages selection allows you to view a historical list of all system messages. To view the messages that your permissions entitle you to see select **System** > **Log Messages**. You will see a display of the messages similar to those shown in Figure 129.

Figure 129 — Log Messages Sample



Log Messages

☑ Date/Time Filter Start 2/19/2014 12:00 AM End 2/20/2014 12:00 AM UTC -05:00

Drag a column header and drop it here to group by that column

Event	Date/Time	Source	Description	Device	Domain
ⓘ	2/19/2014 4:17:15 PM UTC-05:00	LPRInterface::Fixed Camera 1	starting...	Fixed FCU	Administrative
❗	2/19/2014 4:17:07 PM UTC-05:00	LPRPumaInterface::LEFT	LPR did not respond in time...	Puma Car	Alarm Tests
❗	2/19/2014 4:17:07 PM UTC-05:00	LPRPumaInterface::RIGHT	LPR did not respond in time...	Puma Car	Alarm Tests
❗	2/19/2014 4:16:34 PM UTC-05:00	LPRPumaInterface::LEFT	LPR did not respond in time...	Puma Car	Alarm Tests
❗	2/19/2014 4:16:34 PM UTC-05:00	LPRPumaInterface::RIGHT	LPR did not respond in time...	Puma Car	Alarm Tests
❗	2/19/2014 4:16:19 PM UTC-05:00	LPRInterface::Fixed Camera 2	Fixed Camera 2::ControlThr...	Fixed FCU	Administrative
ⓘ	2/19/2014 4:16:19 PM UTC-05:00	LPRInterface::Fixed Camera 2	stopped.	Fixed FCU	Administrative
❗	2/19/2014 4:16:06 PM UTC-05:00	LPRInterface::Fixed Camera 1	Fixed Camera 1::ControlThr...	Fixed FCU	Administrative
ⓘ	2/19/2014 4:16:06 PM UTC-05:00	LPRInterface::Fixed Camera 1	stopped.	Fixed FCU	Administrative

Referring to Figure 130, the user can filter the display in the same ways that you can any other display in EOC, by time, date, time zone offset, and columns. Event filtering is limited to the list of events as displayed in the Event Filter dropdown.

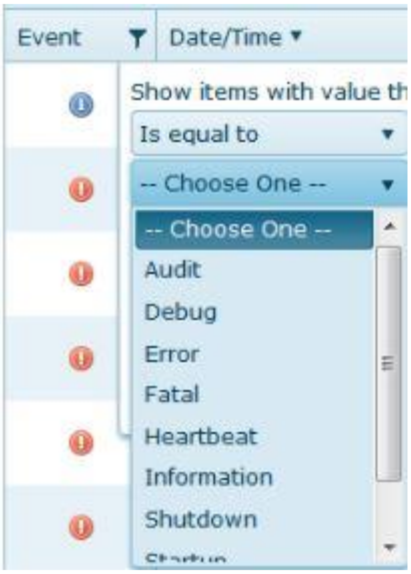
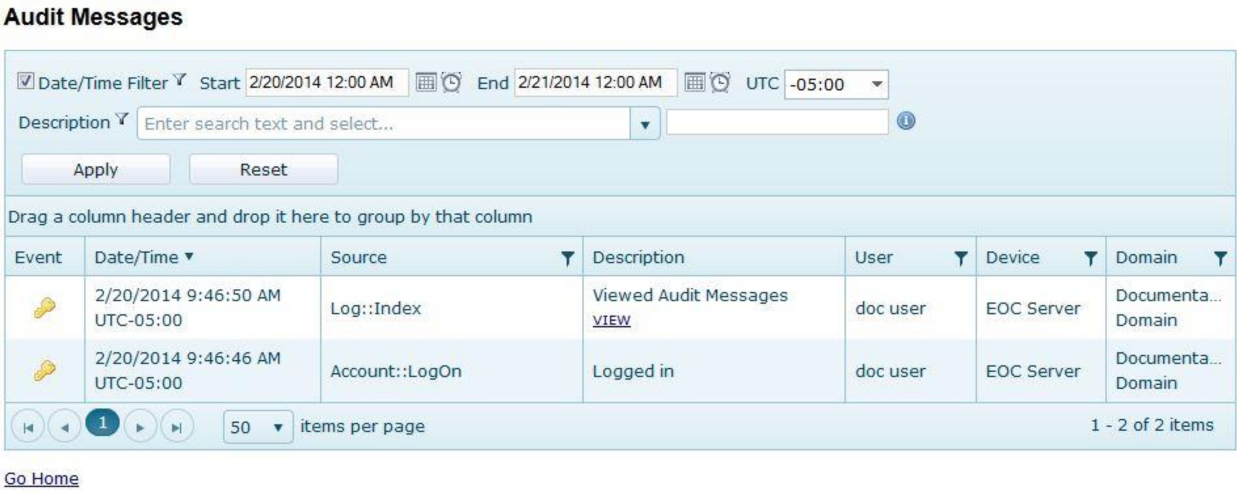


Figure 130 — Event Filtering Sample

Audit Messages

The **Audit Messages** selection allows you to view a historical list of all system activities and who performed them. See Figure 131.



Audit Messages

☑ Date/Time Filter Start 2/20/2014 12:00 AM End 2/21/2014 12:00 AM UTC -05:00

Description Enter search text and select...

Apply Reset

Drag a column header and drop it here to group by that column

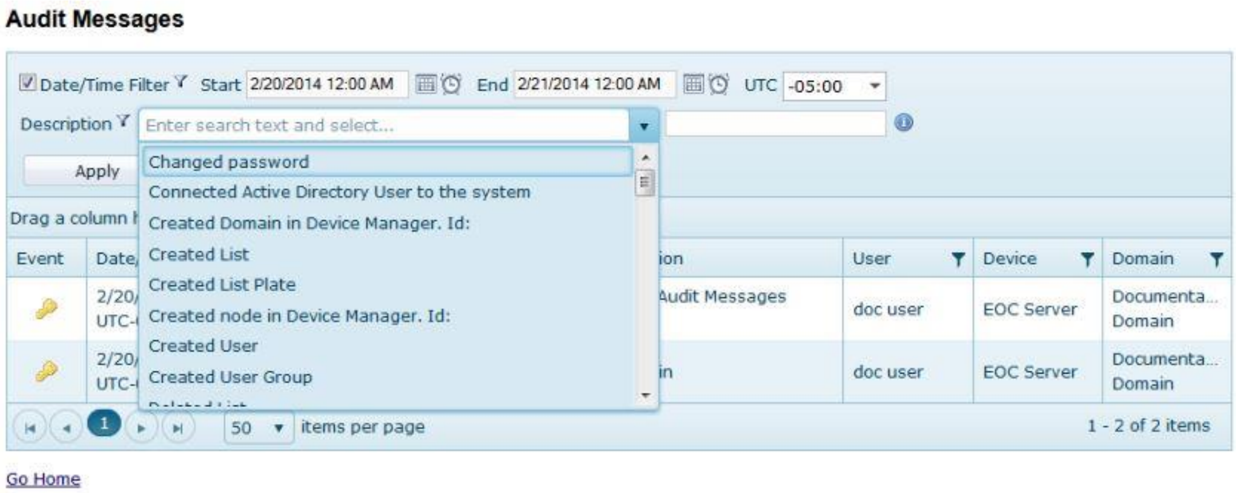
Event	Date/Time	Source	Description	User	Device	Domain
	2/20/2014 9:46:50 AM UTC-05:00	Log::Index	Viewed Audit Messages VIEW	doc user	EOC Server	Documenta... Domain
	2/20/2014 9:46:46 AM UTC-05:00	Account::LogOn	Logged in	doc user	EOC Server	Documenta... Domain

1 50 items per page 1 - 2 of 2 items

Go Home

Figure 131 — Audit Messages Initial Screen

Figure 132 shows the description drop down for the list of what is recorded as Audits.



Audit Messages

☑ Date/Time Filter Start 2/20/2014 12:00 AM End 2/21/2014 12:00 AM UTC -05:00

Description Enter search text and select...

- Changed password
- Connected Active Directory User to the system
- Created Domain in Device Manager. Id:
- Created List
- Created List Plate
- Created node in Device Manager. Id:
- Created User
- Created User Group

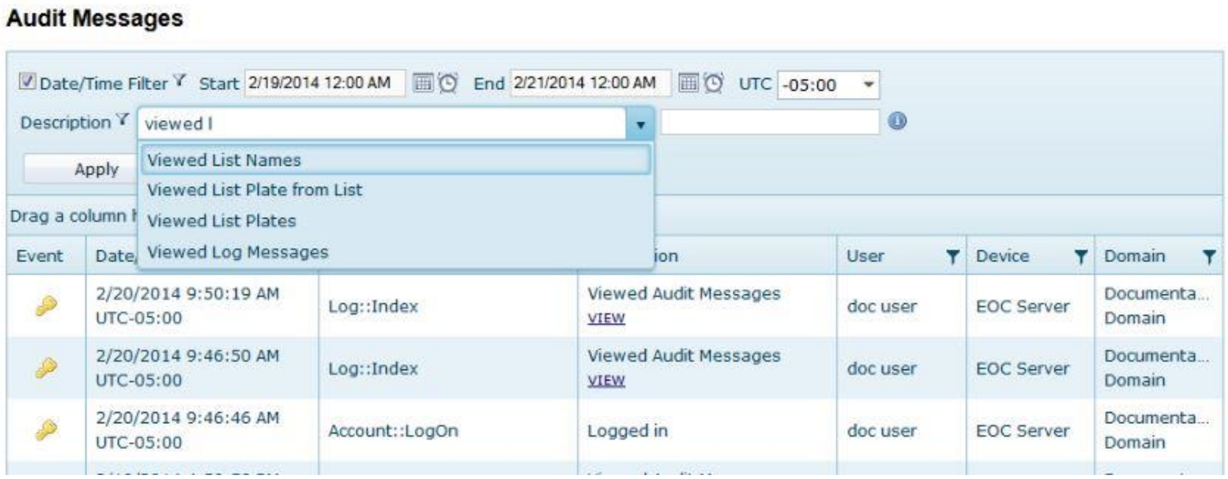
Event	Date,	ion	User	Device	Domain
	2/20/ UTC-	Audit Messages	doc user	EOC Server	Documenta... Domain
	2/20/ UTC-	in	doc user	EOC Server	Documenta... Domain

50 items per page 1 - 2 of 2 items

Go Home

Figure 132 — Audit Messages Description Drop Down

Referring to Figure 133, the user can type a description in the Information Input Field to filter the list and then select an option.



Audit Messages

☑ Date/Time Filter Start 2/19/2014 12:00 AM End 2/21/2014 12:00 AM UTC -05:00

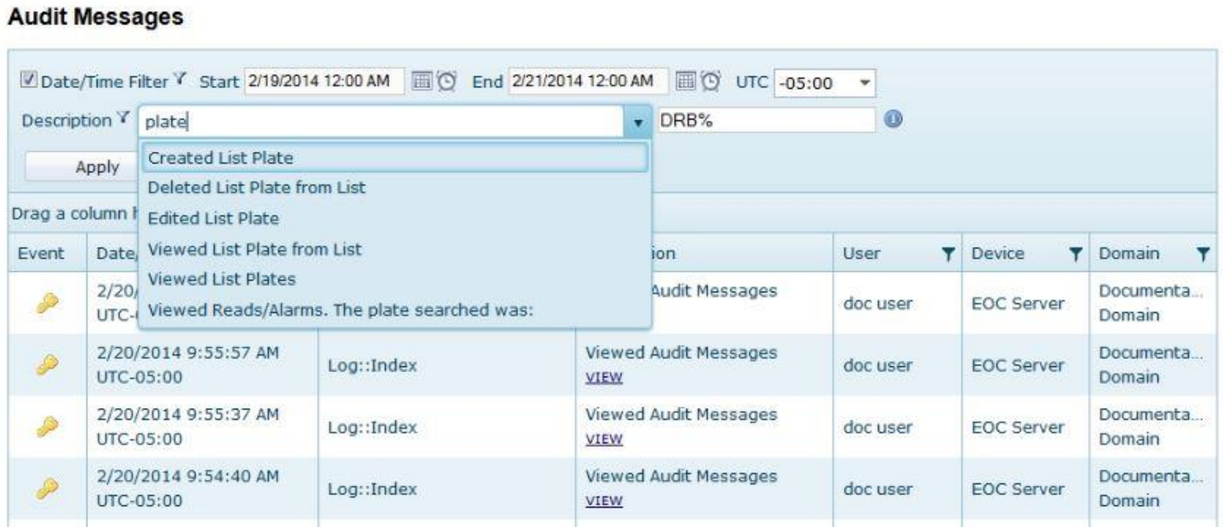
Description viewed l

- Viewed List Names
- Viewed List Plate from List
- Viewed List Plates
- Viewed Log Messages

Event	Date,		ion	User	Device	Domain
	2/20/2014 9:50:19 AM UTC-05:00	Log::Index	Viewed Audit Messages VIEW	doc user	EOC Server	Documenta... Domain
	2/20/2014 9:46:50 AM UTC-05:00	Log::Index	Viewed Audit Messages VIEW	doc user	EOC Server	Documenta... Domain
	2/20/2014 9:46:46 AM UTC-05:00	Account::LogOn	Logged in	doc user	EOC Server	Documenta... Domain

Figure 133 — Audit Messages Information Input Field

Referring to Figure 134, the “empty box” can be used to search for specific items. Figure 134 shows an example of filtering the Description option to “plate” and a plate starting with DRB.



Audit Messages

☑ Date/Time Filter Start 2/19/2014 12:00 AM End 2/21/2014 12:00 AM UTC -05:00

Description plate DRB%

Apply

Created List Plate
Deleted List Plate from List
Edited List Plate
Viewed List Plate from List
Viewed List Plates
Viewed Reads/Alarms. The plate searched was:

Drag a column h

Event	Date,		ion	User	Device	Domain
	2/20/ UTC-(		Audit Messages	doc user	EOC Server	Documenta... Domain
	2/20/2014 9:55:57 AM UTC-05:00	Log::Index	Viewed Audit Messages VIEW	doc user	EOC Server	Documenta... Domain
	2/20/2014 9:55:37 AM UTC-05:00	Log::Index	Viewed Audit Messages VIEW	doc user	EOC Server	Documenta... Domain
	2/20/2014 9:54:40 AM UTC-05:00	Log::Index	Viewed Audit Messages VIEW	doc user	EOC Server	Documenta... Domain

Figure 134 — Audit Messages Description Filtering

Application Settings

General

- **Language**

  The culture used by the application. If set to **Auto Detect**, the setting is taken from the browser.

- **Default Map Latitude and Longitude**

  Sets the default map location when Cross Search, Convoy Search, TOC or Dispatcher maps are displayed.

- **Default Convoy Search Interval**

  Enables the modification of the default plus or minus time Convoy Search uses.

- **TOC Active Alarm Duration (secs)**

  Enables the modification of the default time period TOC uses to keep a recent alarm active. This helps when an alarm is delayed from reaching the EOC in a timely manner.

- **Require Reason For Query**

  For auditing purposes, anytime a user queries reads or alarms a reason for the query must be given. The reason is saved with the Audit message.

- ❑ **Alarm Validation in EOC Server Search Results**

  When enabled Alarm validation can be performed at the EOC server level by authorized users.

SMTP

When EOC was installed, the process asked for SMTP settings to configure how EOC would send emails such as password notifications to new users, etc. You can change these settings in this SMTP section.

- ❑ **From Address**
- ❑ **SMTP Server**
- ❑ **Port**
- ❑ **Authentication Settings**
- ❑ **Send Test Email To**

SQL Membership Provider

This section allows the setting of password constraints for EOC running under SQL Server Membership:

- ❑ **Maximum Invalid Password Attempts**
- ❑ **Password Attempt Window (minutes)**
- ❑ **Minimum Required Password Length**
- ❑ **Minimum Required Nonalphanumeric Characters**

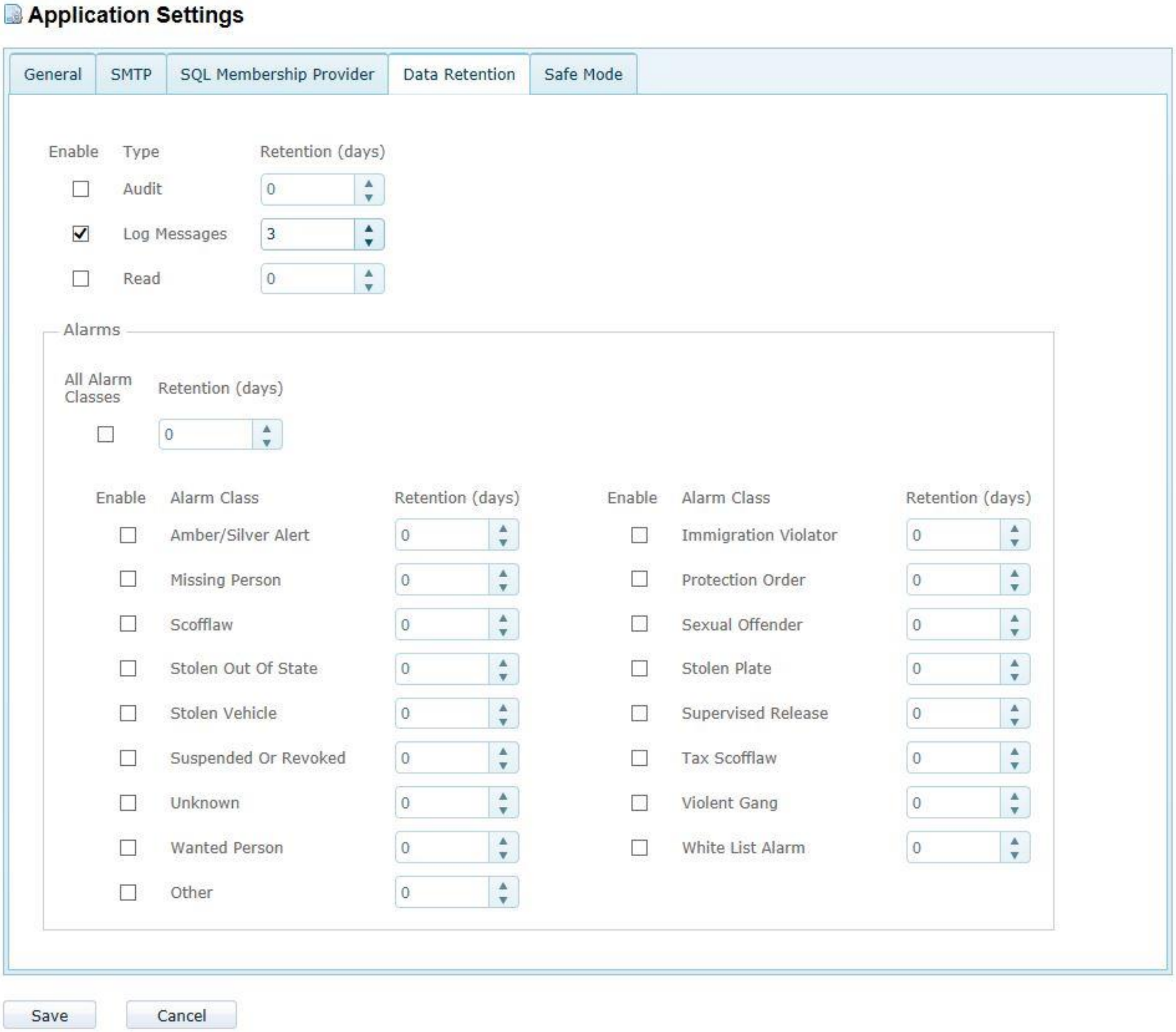
Data Retention

Data Retention parameters are options for setting how many days data is retained/stored in EOC. Users might have different data retention policies for reads or alarms and require to set their own.

Referring to Figure 135, Data Retention can be enabled.

- If there are no limits on Data Retention, uncheck all the Enabled checkboxes.
- Audit, Log Messages and Reads can have their own Data Retention values.
- Alarm retention can be limited in two ways:
  - If all Alarm Types have the same retention policy, select the “All Alarm Classes” checkbox and set the number of days.
  - If different Alarm types have different retention policies, make sure the “All Alarm Classes” checkbox is not selected. Then “Enable” and set each Alarm Type to the appropriate number of retention days.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.



Application Settings

Enable	Type	Retention (days)
□	Audit	0
☑	Log Messages	3
□	Read	0

Alarms

All Alarm Classes	Retention (days)
□	0

Enable	Alarm Class	Retention (days)	Enable	Alarm Class	Retention (days)
□	Amber/Silver Alert	0	□	Immigration Violator	0
□	Missing Person	0	□	Protection Order	0
□	Scofflaw	0	□	Sexual Offender	0
□	Stolen Out Of State	0	□	Stolen Plate	0
□	Stolen Vehicle	0	□	Supervised Release	0
□	Suspended Or Revoked	0	□	Tax Scofflaw	0
□	Unknown	0	□	Violent Gang	0
□	Wanted Person	0	□	White List Alarm	0
□	Other	0			

Figure 135 — Data Retention

Safe Mode

- **Enter and Leave Safe Mode**

  Safe mode use was described in the ***Troubleshooting Using Safe Mode*** section on Page 29.

- **Membership Provider: SQL or Active Directory**

  Allows the conversion of the user Membership Provider to/from SQL Server Mode to/from Active Directory Mode. If EOC is already in Active Directory Mode, you can review the Active Directory settings for Connection String, Network Domain and Username.

- **Changing from SQL Server Mode to Active Directory Mode**

  There are prerequisites for converting to Active Directory Mode, both for the EOC Server machine and for each CarSystem installation that will operate in Active Directory Mode.

  - **EOC Server Side**
    - The LDAP Server must be hosted using Microsoft Active Directory.
    - All EOC users must be in one LDAP directory tree.
    - An LDAP connection string must be established, including host, port and protocol that points to the relevant Users container. For example:

      LDAP://ds1.example.com/CN=Users,DC=example,DC=com
    - You must have an LDAP login username and password.
    - Set firewall access to the LDAP server to either **Unencrypted connection on TCP/389** or **Implicit SSL Encryption connection on TCP/636**.
    - **NOTE**: Queries of the Global Catalog are not supported.

  - **CarSystem Installations**

    Each CarSystem installation that will be used in Active Directory Mode must meet the following requirements:

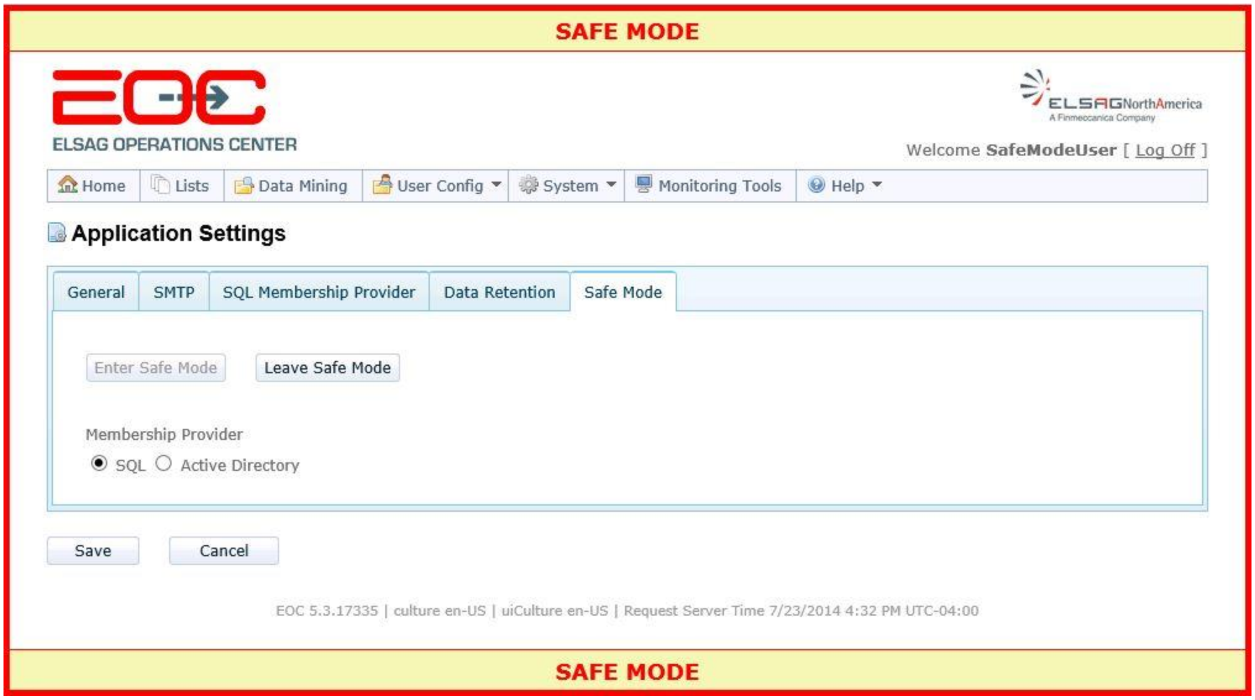
    - The CarSystem computer must be attached to the LDAP server's Active Directory domain or on a domain in the same domain forest. A trusted domain will also work.
    - The user in Car System must have log in permission on the client computer.
    - The CarSystem user must have either network access to the domain controller at login time or must be able to use cached credentials. (These are standard requirements for Windows Active Directory logins.)
    - CarSystem will automatically authenticate using the credentials that the Active Directory user logged into Windows with or as a specific user when used with the **Run As...** command.

  Once you've made sure that all the prerequisite software and IIS settings are correct on your computer, you can convert the EOC 5.x server to Active Directory Mode.

Follow these steps to change the EOC to Active Directory Mode:

(1) Follow the instructions for entering Safe Mode in the *Accessing Safe Mode from within EOC* on Page 29.

(2) Referring to Figure 136, navigate to **System** > **App Settings** > **Safe Mode** tab.

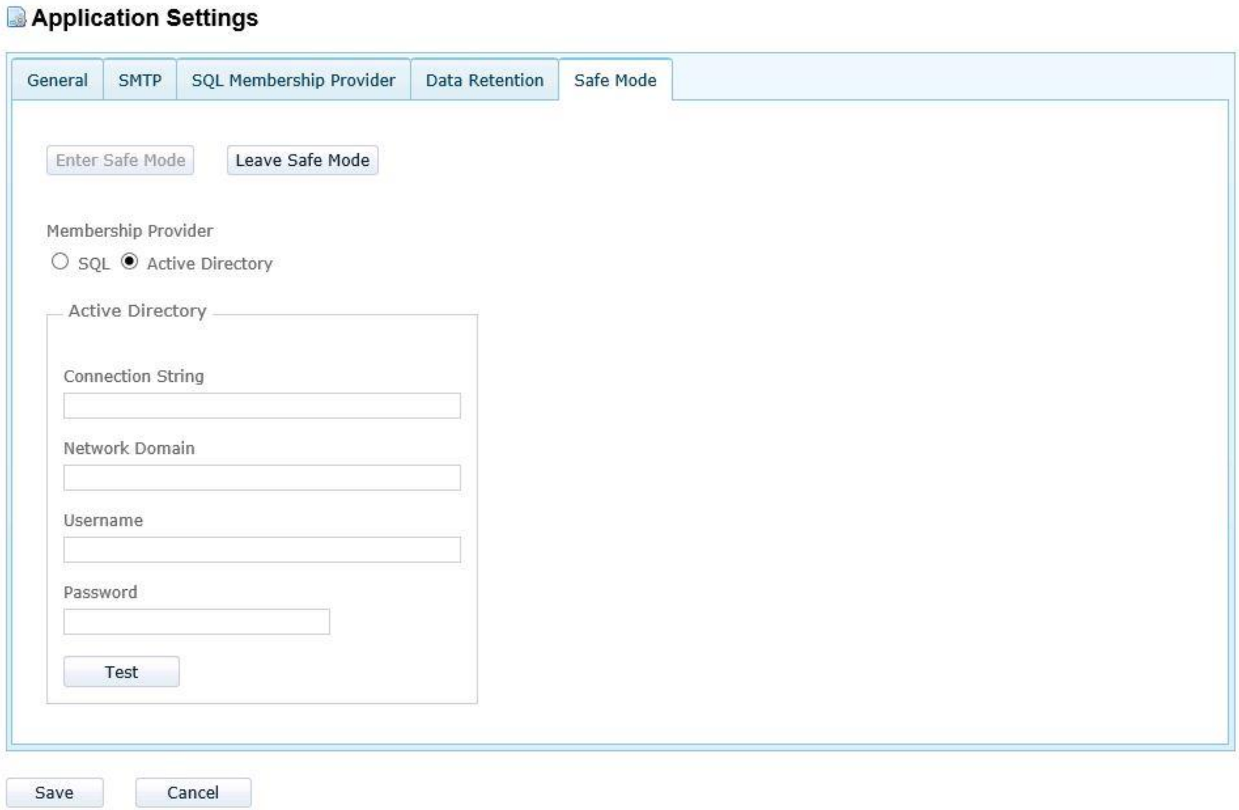


Membership Provider
● SQL ○ Active Directory

EOC 5.3.17335 | culture en-US | uiCulture en-US | Request Server Time 7/23/2014 4:32 PM UTC-04:00

Figure 136 — Application Settings Safe Mode Tab

(3) Referring to Figure 137, select the Active Directory radio button which will display the fields needed to switch to Active Directory Mode.



Application Settings

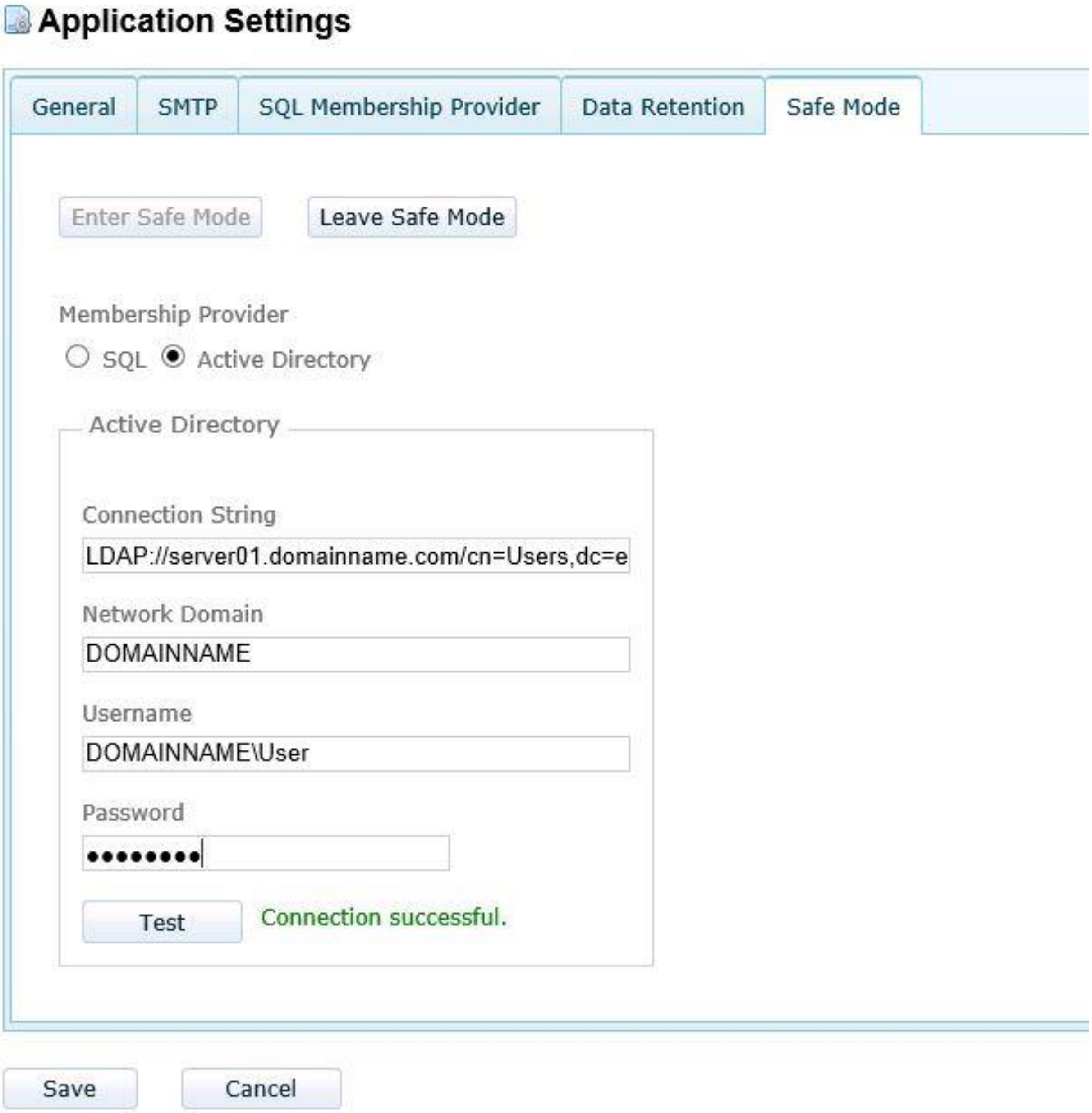
Membership Provider

○ SQL ● Active Directory

Figure 137 — Membership Provider Active Directory Entry

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(4) Referring to Figure 138, enter the required information and click the **Test** button.



Application Settings

Membership Provider

○ SQL ● Active Directory

Active Directory

Connection String

LDAP://server01.domainname.com/cn=Users,dc=e

Network Domain

DOMAINNAME

Username

DOMAINNAME\User

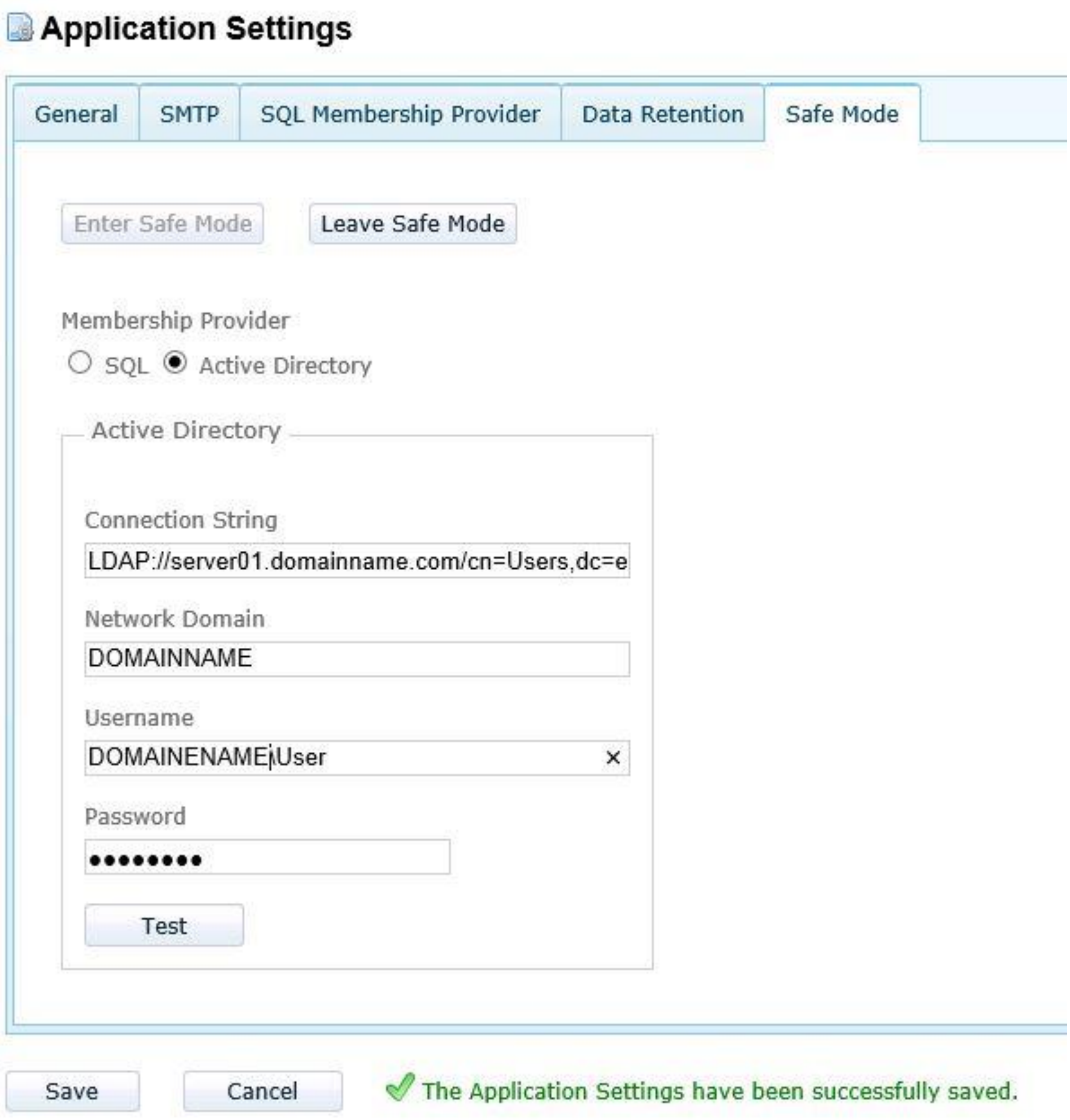
Password

●●●●●●●●●

Connection successful.

Figure 138 — Active Directory Test Successful

(5) Referring to Figure 139, click **Save** if you receive the “**Connection Successful**” message. If the “**Connection Successful**” message is not displayed, make any corrections necessary to successfully test the settings.



Application Settings

Membership Provider

○ SQL ● Active Directory

Active Directory

Connection String: LDAP://server01.domainname.com/cn=Users,dc=e

Network Domain: DOMAINNAME

Username: DOMAINENAME\User

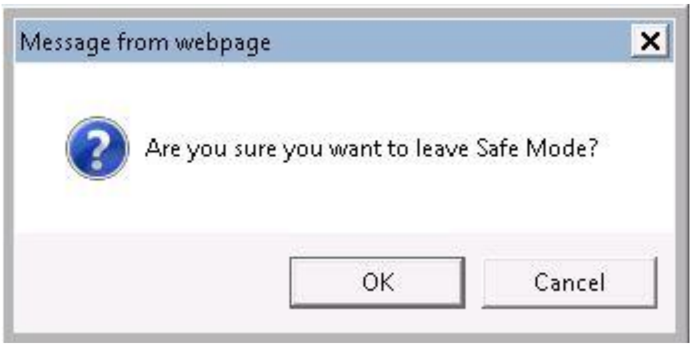
Password: ••••••••

✓ The Application Settings have been successfully saved.

Figure 139 — Active Directory Settings Saved

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

(6) Referring to Figure 140, click the **Leave Safe Mode** button and acknowledge that you want to leave safe mode.



Message from webpage

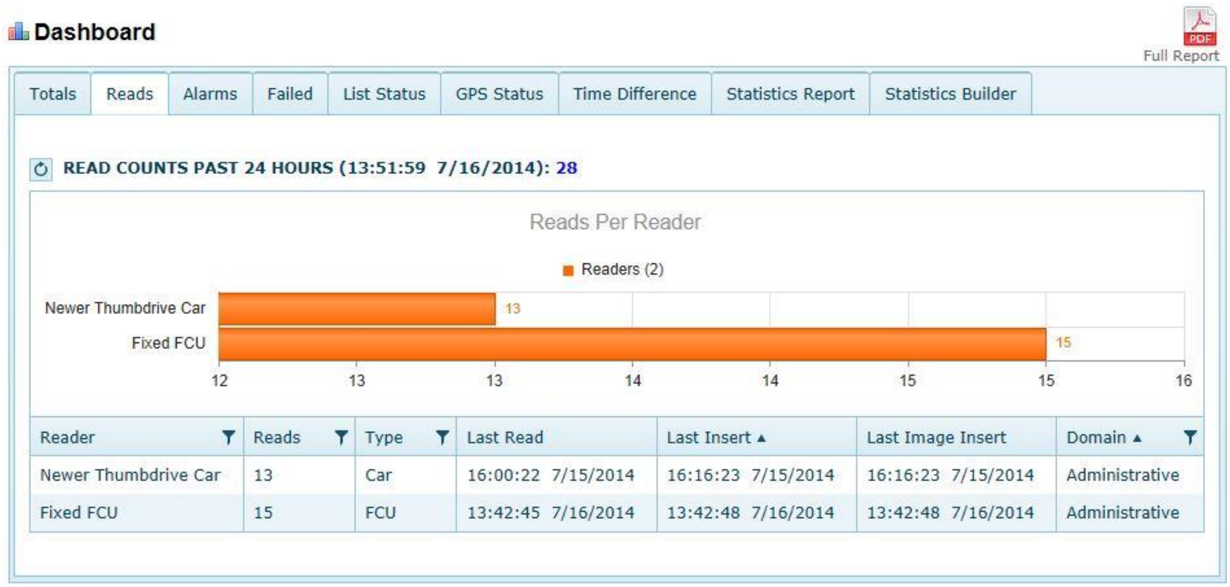
Are you sure you want to leave Safe Mode?

Figure 140 — Leave Safe Mode Confirmation

Chapter 8 — Monitoring Tools

Dashboard

Referring to Figure 141, select **Monitoring Tools > Dashboard** on the menu bar. Dashboard is a utility for system administrators and technicians that need to observe current performance details of the EOC system.



READ COUNTS PAST 24 HOURS (13:51:59 7/16/2014): 28

Reader	Reads	Type	Last Read	Last Insert ▲	Last Image Insert	Domain ▲
Newer Thumbdrive Car	13	Car	16:00:22 7/15/2014	16:16:23 7/15/2014	16:16:23 7/15/2014	Administrative
Fixed FCU	15	FCU	13:42:45 7/16/2014	13:42:48 7/16/2014	13:42:48 7/16/2014	Administrative

Figure 141 — Dashboard Reads Display

The Dashboard Tabs are described below:

Totals: Shows graph and statistics for:

- Total Read count since EOC started
- Total Reads during the last minute, and
- Read Count totals for the last two days.

Reads: Shows graph and statistics by Reader for the Read counts in the last 24 hours. Referring to Figure 141, the information shown per Reader is reader Type, Last Read Time, EOC Read and Image Insert times sorted by Domain by Last EOC Insert Time.

Alarms: Shows graph and statistics by Reader for the Alarm counts in the last 24 hours. This excludes Suspended or Revoked Registration alarms.

Failed: Readers that failed to report in the last hour. These would be cars and FCUs only.

List Status: All Lists and their success/failure status if they have an automated import task.

GPS Status: Graph and statistics by Reader for bad GPS coordinates (zeros) sorted by Domain by percentage of bad GPS coordinates for the last two weeks.

Time Difference: Shows Car and FCU system time differences compared to the EOC server time.

Statistics Report: Shows reader statistics grouped by reader for the last 8 days (default), number of reads, accepted or rejected alarms and domain. Results can be exported in CSV format.

Statistics Builder: Read Rate, Image Insert Rate and Alarm Rate can be compared for back log detection by all or any reader for the same or different time periods. Use examples are graphical comparison of Read data to Image data flow into EOC or weekly comparison of Read Rates. Helpful shortcut buttons allow quick display of All Readers Read Rate for Today, This Week or Last Week. Results can be exported in CSV format. This replaced Reader Analysis.

The Dashboard PDF Full Report icon will export a formatted PDF report for the Totals, Reads, Alarms, Failed, List Status, GPS Status and Time Difference results. Statistics Report and Builder have their own CSV exports.

Statistics Report

Statistic Report allows the user to do the following:

- Displays statistics per car/reader for date, number of reads, accepted or rejected alarms and domain
- Creates data sets of statistics using filters for reader, date, number of reads, accepted or rejected alarms and domain

Exports data sets of statistics to comma-separated value (CSV) files. You can use the EOC to inspect the statistics for reads and alarms collected by the Readers that are feeding data to the EOC. (A Reader is the EOC’s term for the source of all cameras associated with a particular car or FCU.) To view statistics, perform the following steps:

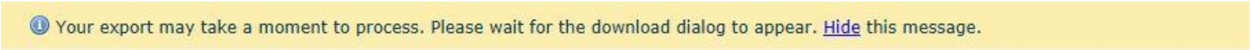
You can use the filtering mechanisms in the other columns to view the data in many different ways.

Exporting Statistics Report

You can also export statistical reports from the application to a Comma-Separated Value (CSV) file.

To do this, first create the data set that you want to export, as shown above. Once you’ve done that, follow this procedure:

(1) Press the CSV icon and referring to Figure 142, you will see this dialog screen:

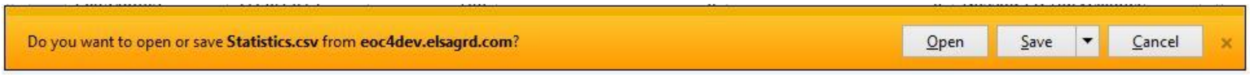


ⓘ Your export may take a moment to process. Please wait for the download dialog to appear. Hide this message.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

Figure 142 — Export Dialog

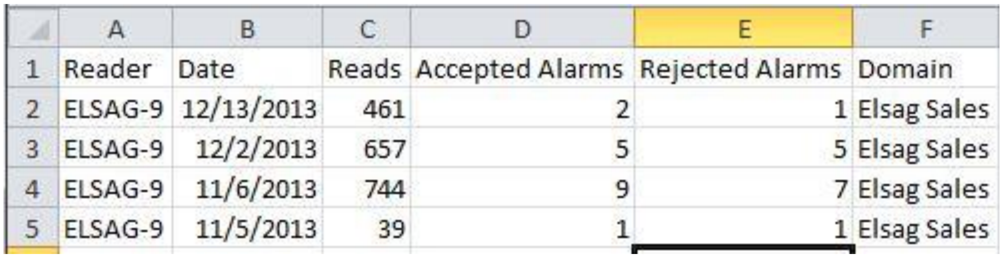
(2) Referring to Figure 143, the system will download the data, and then Windows will prompt you to open or save the CSV file. By default, the file will be saved in your Windows **Downloads** folder:



Do you want to open or save **Statistics.csv** from **eoc4dev.elsagrd.com**?

Figure 143 — Open or Save Dialog

(3) If you open the CSV file, it will display in Excel and look like Figure 144.



	A	B	C	D	E	F
1	Reader	Date	Reads	Accepted Alarms	Rejected Alarms	Domain
2	ELSAG-9	12/13/2013	461	2	1	Elsag Sales
3	ELSAG-9	12/2/2013	657	5	5	Elsag Sales
4	ELSAG-9	11/6/2013	744	9	7	Elsag Sales
5	ELSAG-9	11/5/2013	39	1	1	Elsag Sales

Figure 144 — Exported Statistics Report CSV File Displayed

Statistics Builder

Statistic Builder allows the user to do the following:

- Displays Read Rate, Image Insert Rate and Alarm Rate statistics for all Readers, one Reader or multiple Readers using variable Start Dates
- Read Rate, Image Insert Rate and Alarm Rate can be compared for back log analysis by all or any reader for the same or different time periods.

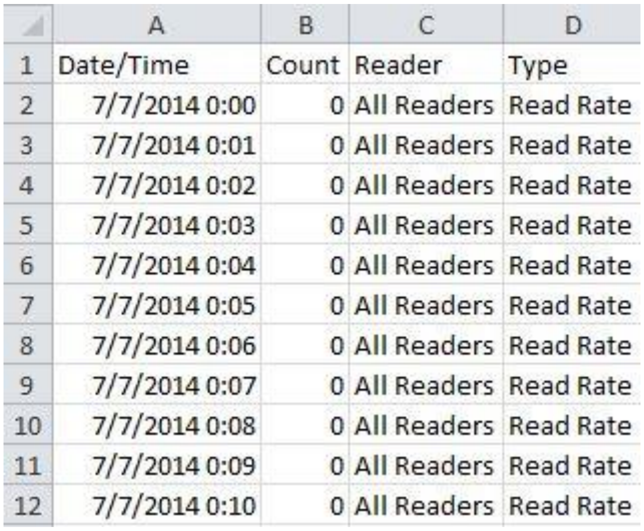
Use examples are graphical comparison of Read data to Image data flow into EOC or weekly comparison of Read Rates or comparing Read Rate to Image Insert Rate to review image back logs (delayed image transmission to the EOC).

Helpful shortcut buttons allow quick display of All Readers Read Rate for Today, This Week or Last Week. Results can be exported in CSV format. This replaced Reader Analysis

Exporting Statistics Builder

You can also export the Statistics Builder results from the application to a Comma-Separated Value (CSV) file.

To do this, first create the data set that you want to export, as shown above. Once you’ve done that, follow the same Exporting Statistics Report procedures on Page 146. If you open the CSV file, it will display in Excel and look like Figure 145.



	A	B	C	D
1	Date/Time	Count	Reader	Type
2	7/7/2014 0:00	0	All Readers	Read Rate
3	7/7/2014 0:01	0	All Readers	Read Rate
4	7/7/2014 0:02	0	All Readers	Read Rate
5	7/7/2014 0:03	0	All Readers	Read Rate
6	7/7/2014 0:04	0	All Readers	Read Rate
7	7/7/2014 0:05	0	All Readers	Read Rate
8	7/7/2014 0:06	0	All Readers	Read Rate
9	7/7/2014 0:07	0	All Readers	Read Rate
10	7/7/2014 0:08	0	All Readers	Read Rate
11	7/7/2014 0:09	0	All Readers	Read Rate
12	7/7/2014 0:10	0	All Readers	Read Rate

Figure 145 — Exported Statistics Builder CSV File Displayed

Statistics Builder export results are per minute results compared to the Statistics Report results which are per day.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

TOC — Tactical Operation Center

The Tactical Operations Center (TOC) EOC plug-in feature displays recent alarms. Alarms generated from cars or fixed cameras feed back to the EOC server, which populate the most recent alarms list on the TOC screen.

Mobile clients which have wireless access to the EOC can access the TOC screen through a web browser.

To view TOC perform the steps that follow:

(1) Select **Monitoring Tools > TOC** from the Monitoring selection on the menu bar.

(2) A list of all recent alerts will load onto the display. You'll see the screen shown in **Figure** 146.

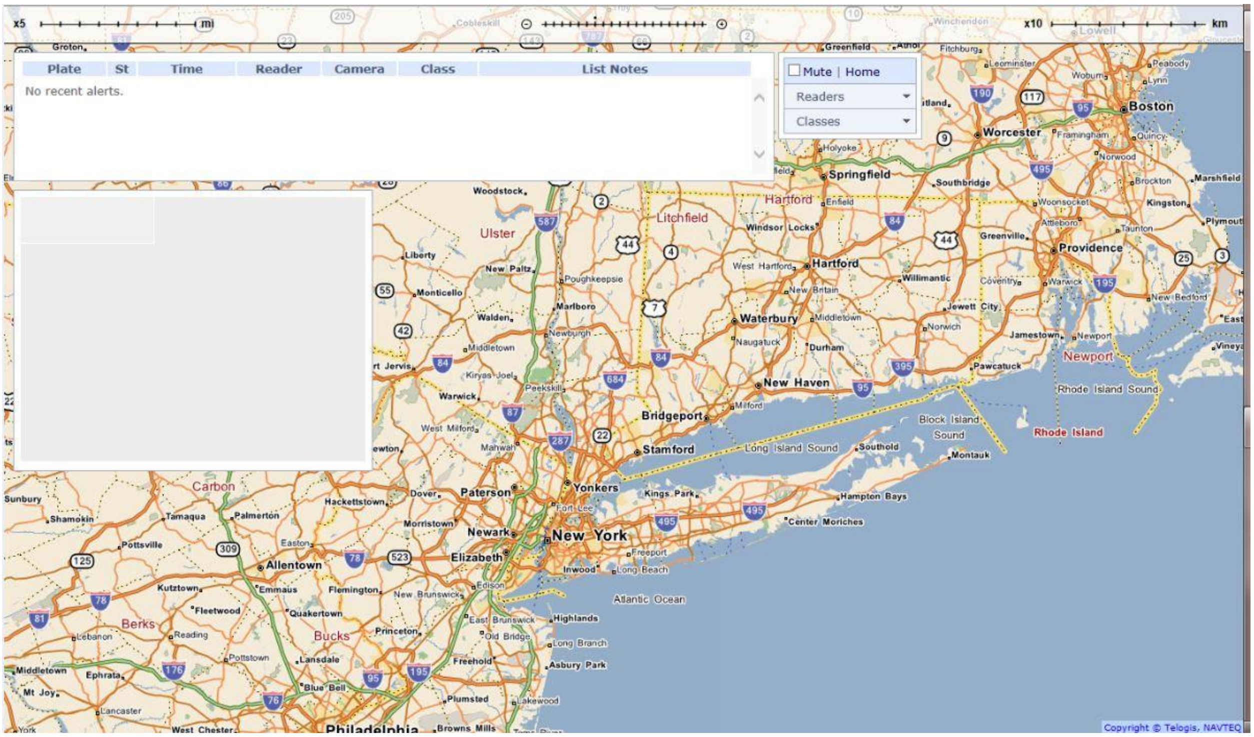


Plate	St	Time	Reader	Camera	Class	List Notes
No recent alerts.						

Figure 146 — TOC Main Screen

(3) When an alarm read comes through, an audible sound will be heard. This can be turned on and off using the **MUTE** feature. The most recent read will be displayed in red for two minutes. A balloon will pop up and show the hit location.

(4) Selecting a specific alert will focus the Alarm showing the vehicle and plate image, and a specific map location. You can also maximize the size of both vehicle and plate image by clicking on them individually.

(5) The user can select a specific reader or multiple readers by using the **Readers Tab** on the right hand side of the screen. See Figure 147.

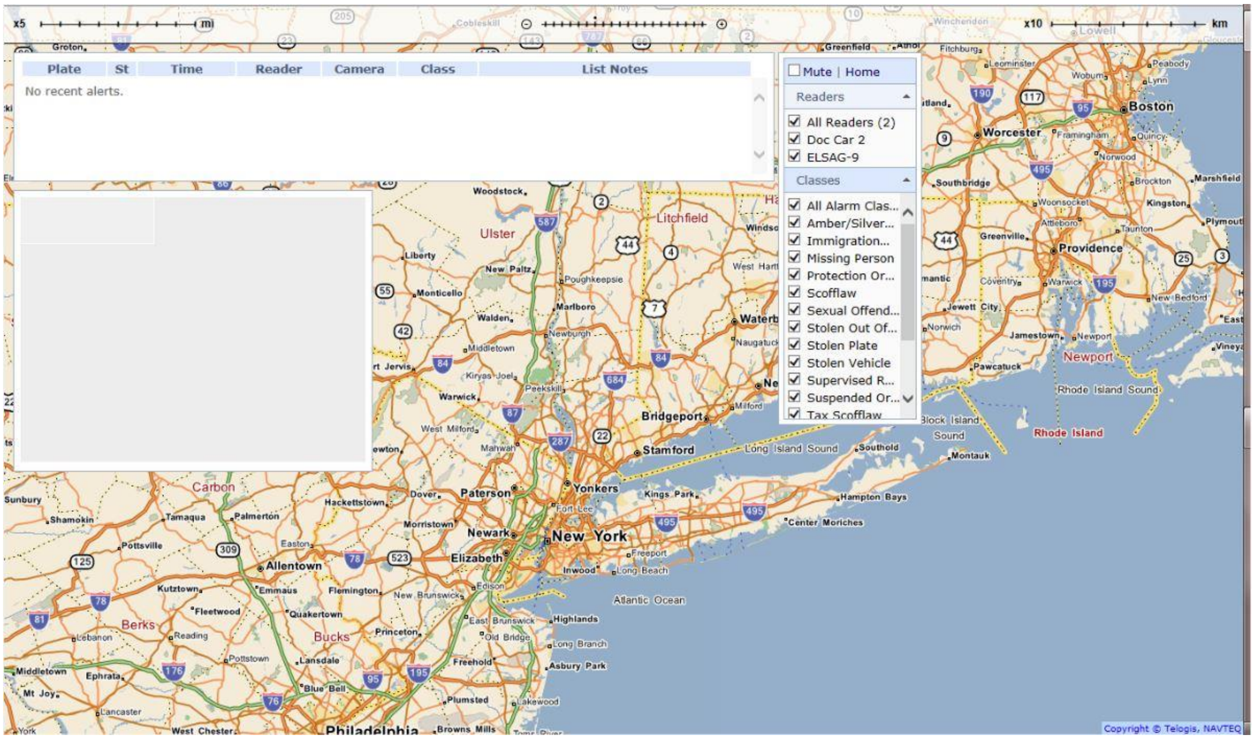


Plate	St	Time	Reader	Camera	Class	List Notes
No recent alerts.						

□ Mute | Home

Readers

☑ All Readers (2)
☑ Doc Car 2
☑ ELSAG-9

Classes

☑ All Alarm Clas...
☑ Amber/Silver...
☑ Immigration...
☑ Missing Person
☑ Protection Or...
☑ Scofflaw
☑ Sexual Offend...
☑ Stolen Out Of...
☑ Stolen Plate
☑ Stolen Vehicle
☑ Supervised R...
☑ Suspended Or...
☑ Tax Scofflaw

Figure 147 — TOC Parameters Screen

(6) The user can also view specific alarm classes by using the **Alarm Classes** tab on the right hand side of the screen.

Dispatcher Plug-In

The EOC Dispatcher allows users to view real-time alarms from camera sites with the ability to Correct/Incorrect each alarm record, Edit and add Officer Notes.

The Dispatcher Plug-In feature allows EOC users to monitor and acknowledge Alarms from remote cameras connected to ELSAG's CarSystem which have not been confirmed in the field as correct or incorrect. This is particularly helpful for Alarms from fixed, unmanned cameras. Dispatcher consists of three elements:

- CarSystem — the source of alarms, included with a CarSystem implementation in a vehicle or Fixed Site (FCU) equipped with LPR cameras
- EOC Server — ELSAG Operations Center, and
- Dispatcher Plug-In — When installed on the EOC, the Dispatcher Web GUI will be available to users to monitor camera sites to which they have permissions.

Figure 148 illustrates the Dispatcher components.

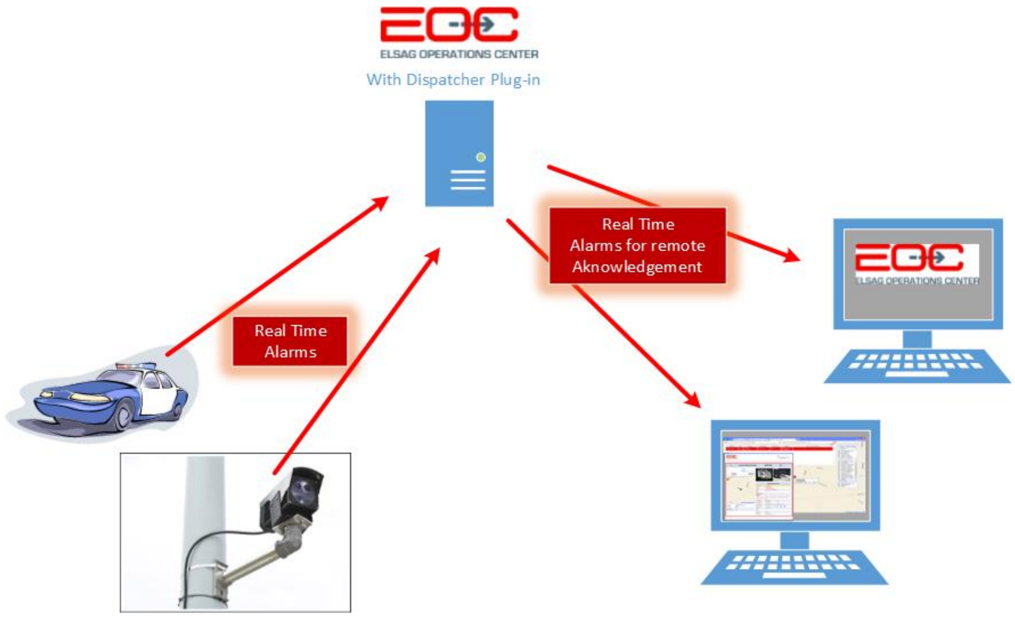


Figure 148 — Dispatcher Component Block Diagram

An alarm originates wherever the CarSystem reader is installed, either from a car or a fixed camera. The alarm is routed into the EOC server, which then redirects it out to various Dispatcher clients. Alarms displayed on each Dispatcher Client is determined by the user's domain permissions.

To open Dispatcher select **Monitoring Tools > Dispatcher** from menu bar.

As shown in Figure 149, a list of all recent alarms will load onto the display.

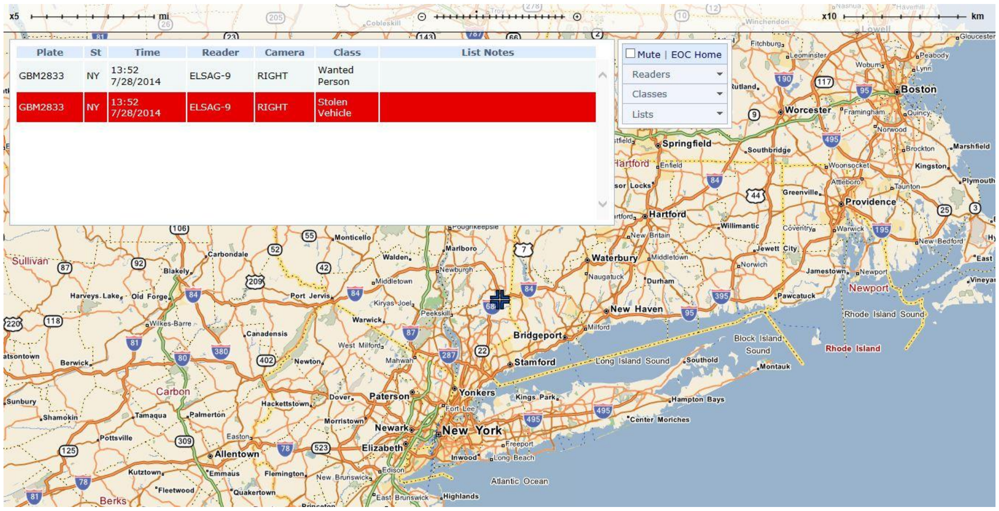


Plate	St	Time	Reader	Camera	Class	List Notes
GBM2833	NY	13:52 7/28/2014	ELSAG-9	RIGHT	Wanted Person	
GBM2833	NY	13:52 7/28/2014	ELSAG-9	RIGHT	Stolen Vehicle	

Figure 149 — Dispatcher Main Screen

When an alarm read comes through, an audible sound will be heard. This can be turned on and off using the **MUTE** feature.

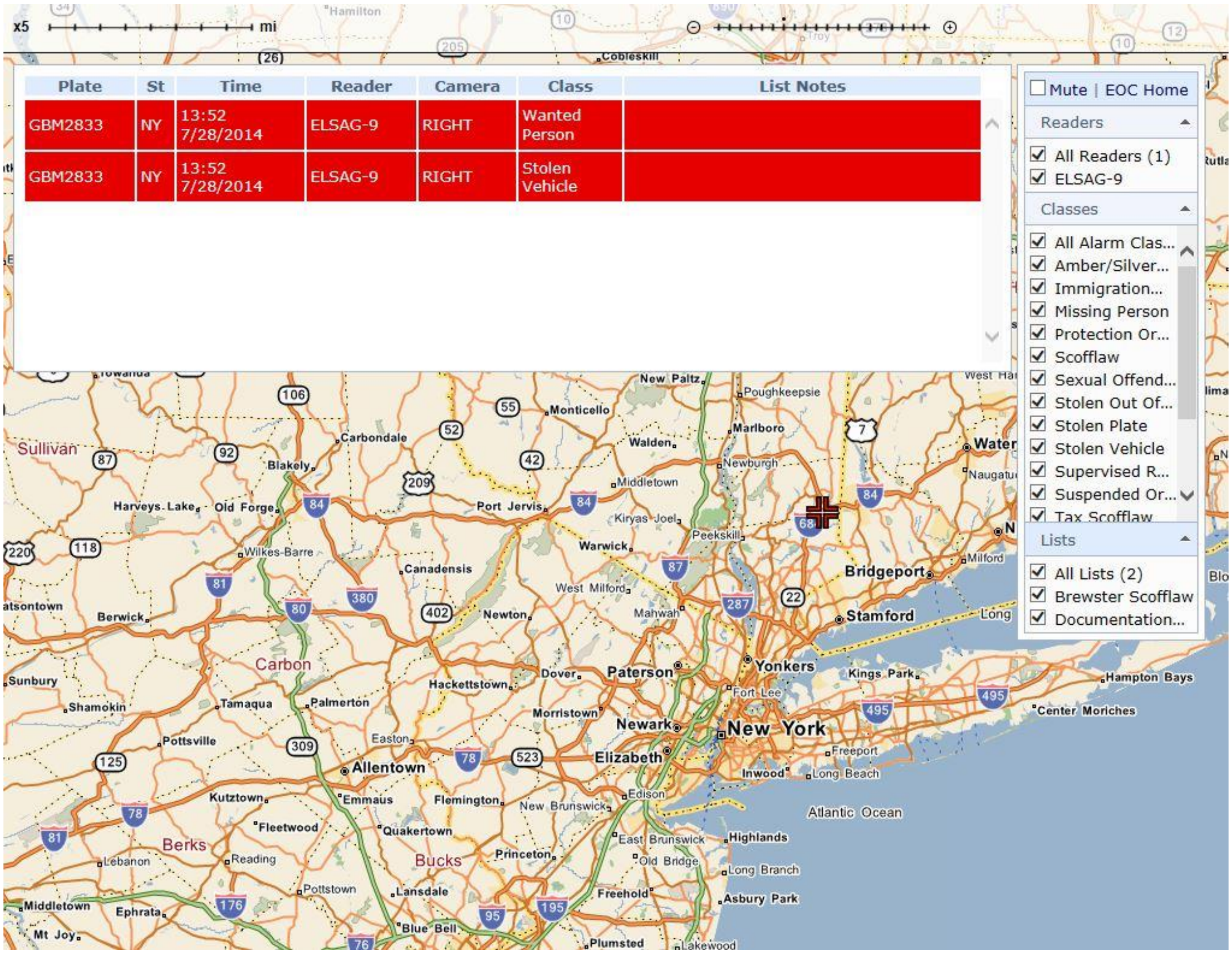


Plate	St	Time	Reader	Camera	Class	List Notes
GBM2833	NY	13:52 7/28/2014	ELSAG-9	RIGHT	Wanted Person	
GBM2833	NY	13:52 7/28/2014	ELSAG-9	RIGHT	Stolen Vehicle	

□ Mute | EOC Home

Readers

☑ All Readers (1)
☑ ELSAG-9

Classes

☑ All Alarm Clas...
☑ Amber/Silver...
☑ Immigration...
☑ Missing Person
☑ Protection Or...
☑ Scofflaw
☑ Sexual Offend...
☑ Stolen Out Of...
☑ Stolen Plate
☑ Stolen Vehicle
☑ Supervised R...
☑ Suspended Or...
☑ Tax Scofflaw

Lists

☑ All Lists (2)
☑ Brewster Scofflaw
☑ Documentation...

Figure 150 — Alarm Location and Parameters

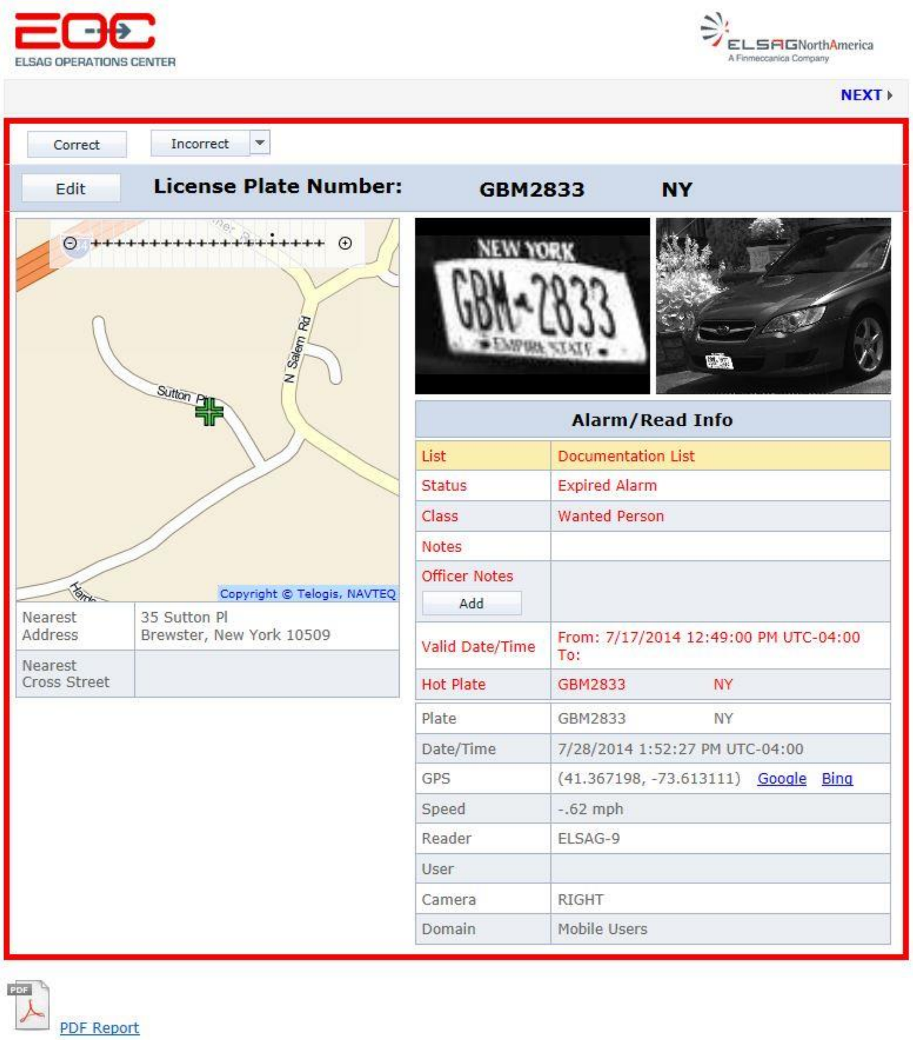
Selecting a specific alert will pop up the Alarm details window showing the vehicle and plate image, and a specific map location. You can also maximize the size of both vehicle and plate image by clicking on them individually.

NOTE: Referring to Figure 150, the user can select a specific reader or multiple readers by using the **Readers Tab** on the right hand side of the screen.

Referring to Figure 150, the user can select a specific alarm class or multiple classes by using the **Alarm Classes Tab** on the right hand side of the screen.

The user can select a specific list source or multiple lists by using the **Lists Tab** on the right hand side of the screen (see Figure 150).

Referring to Figure 150, when an Alarm event is displayed the user can click on the row of that Alarm event causing a pop up window to be displayed. Referring to Figure 151, the detail of the event with images are shown.



License Plate Number: GBM2833 NY

Nearest Address	35 Sutton Pl Brewster, New York 10509
Nearest Cross Street	

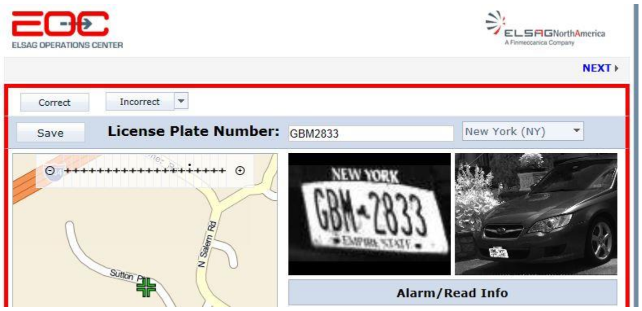
Alarm/Read Info

List	Documentation List
Status	Expired Alarm
Class	Wanted Person
Notes	
Officer Notes	
Valid Date/Time	From: 7/17/2014 12:49:00 PM UTC-04:00 To:
Hot Plate	GBM2833 NY
Plate	GBM2833 NY
Date/Time	7/28/2014 1:52:27 PM UTC-04:00
GPS	(41.367198, -73.613111) Google Bing
Speed	-.62 mph
Reader	ELSAG-9
User	
Camera	RIGHT
Domain	Mobile Users

Figure 151 — Alarm Displayed

In the detail of the Alarm event, users have the ability to:

- Edit the plate read by clicking **Edit**— this option should be used if it was a misread
- Correct or Incorrect the Alarm Event — Correct means the read was correct, Incorrect has different categories that can be selected from the drop down box. See Figure 152 and Figure 153 that follow.



License Plate Number: GBM2833 New York (NY)

Figure 152 — Alarm Event Edit Option (Save)

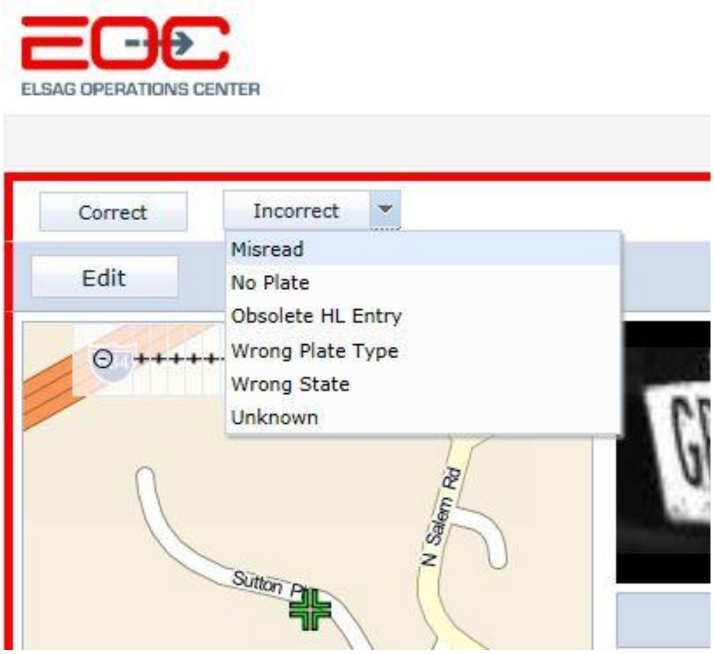


Figure 153 — Alarm Event Incorrect Options

The user can also click the Officer Notes 'Add' button and the screen shown in Figure 154 will appear. This feature allows the user to add additional notes to the Alarm so if this Alarm is monitored again, more information can be shared with other users. Also refer to Figure 155 with Officer Notes Added.

NOTE: Any user of the system will see these notes once these are saved.

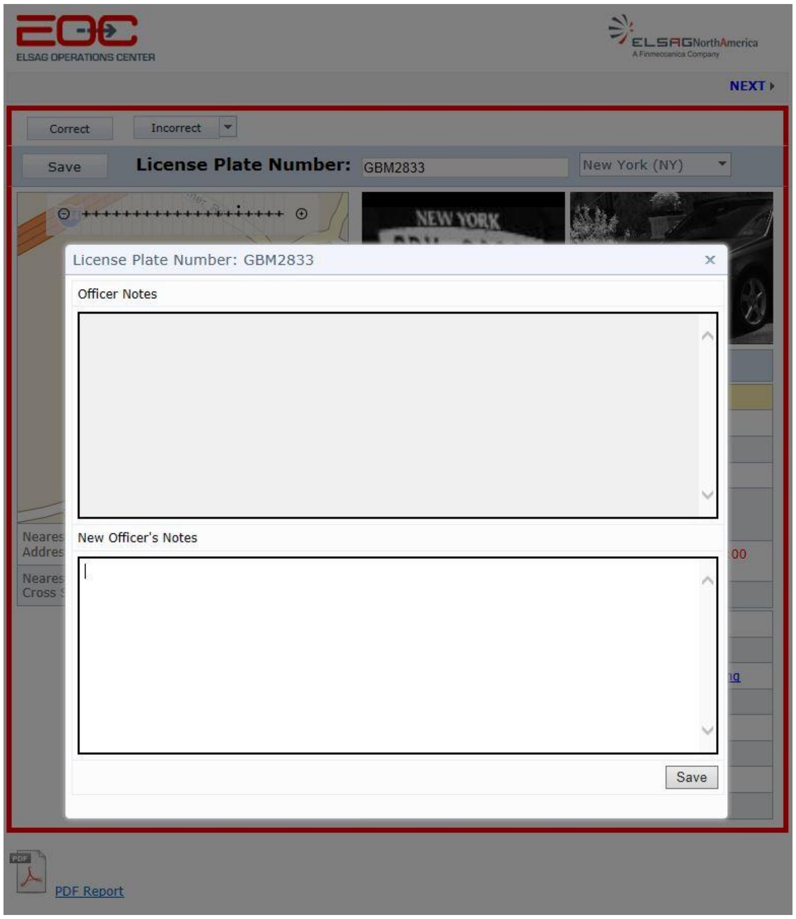
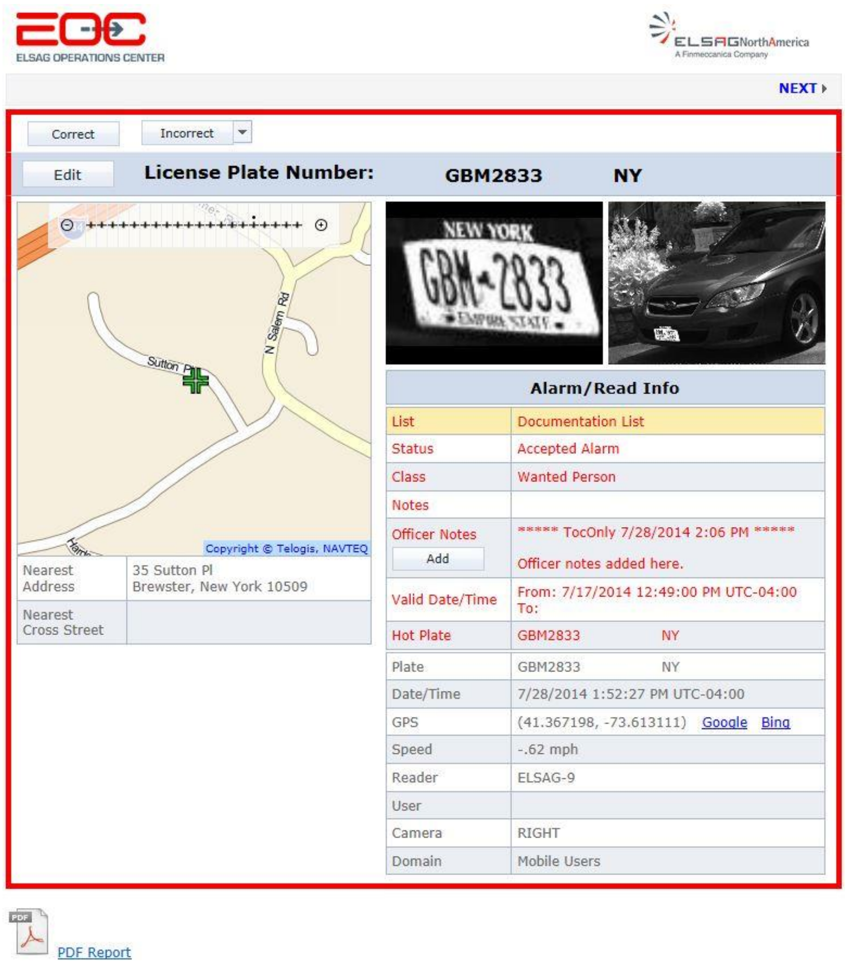


Figure 154 — Add Officer Notes Screen



License Plate Number: GBM2833 NY

Nearest Address	35 Sutton Pl Brewster, New York 10509
Nearest Cross Street	

Alarm/Read Info

List	Documentation List
Status	Accepted Alarm
Class	Wanted Person
Notes	
Officer Notes	***** TocOnly 7/28/2014 2:06 PM ***** Officer notes added here.
Valid Date/Time	From: 7/17/2014 12:49:00 PM UTC-04:00 To:
Hot Plate	GBM2833 NY
Plate	GBM2833 NY
Date/Time	7/28/2014 1:52:27 PM UTC-04:00
GPS	(41.367198, -73.613111) Google Bing
Speed	-.62 mph
Reader	ELSAG-9
User	
Camera	RIGHT
Domain	Mobile Users

Figure 155 — Screen Shown After Officer Notes Added

Help

- **About**
  - Describes the EOC product.

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

NOTES:

NOTES:

NOTES:

Confidential Information — This document contains confidential and proprietary information for customer use only. This information may not be disseminated to any unauthorized individual or entity or for general public release.

ELSAGNorthAmerica
A Finmeccanica Company